(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 989 557 A1

(12) EUROPEAN PATENT APPLICATION

published in accordance with Art. 158(3) EPC

(43) Date of publication:
29.03.2000 Bulletin 2000/13

(21) Application number: **99900674.5**

(22) Date of filing: **25.01.1999**

(51) Int. Cl.[7]: **G11B 20/10**, H04N 5/91

(86) International application number:
PCT/JP99/00292

(87) International publication number:
WO 99/38164 (29.07.1999 Gazette 1999/30)

(84) Designated Contracting States:
DE FR GB

(30) Priority: **26.01.1998 JP 1247498**
09.02.1998 JP 2757298

(71) Applicant:
MATSUSHITA ELECTRIC INDUSTRIAL CO., LTD.
Kadoma-shi, Osaka 571-8501 (JP)

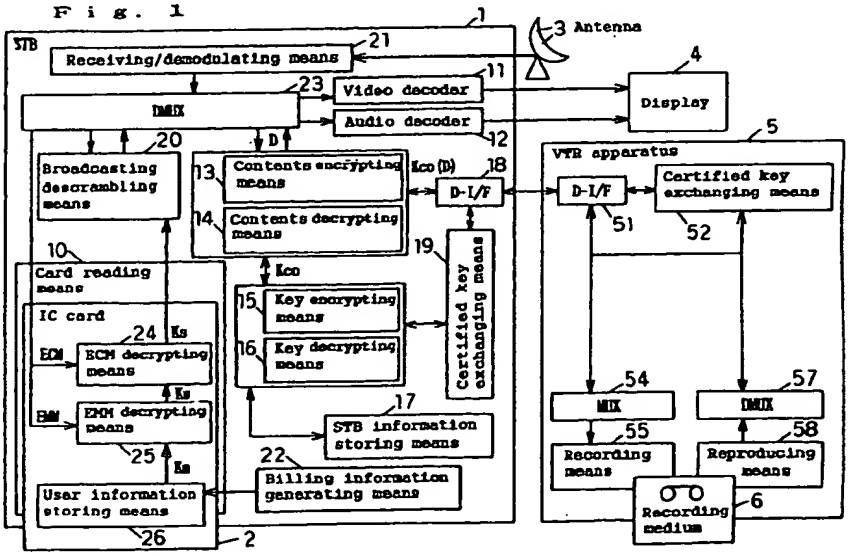
(72) Inventors:
- **YAMADA, Masazumi**
  Osaka 570-0011 (JP)
- **IITSUKA, Hiroyuki**
  Osaka 576-0033 (JP)
- **GOTO, Shoichi**
  Osaka 576-0021 (JP)
- **TAKECHI, Hideaki**
  Room 201
  11-10, Komatsu 4-chome
  Osaka-shi Osaka 533-0004 (JP)

(74) Representative:
Schuster, Thomas, Dipl.-Phys.
Grünecker, Kinkeldey, Stockmair & Schwanhäusser
Anwaltssozietät
Maximilianstrasse 58
80538 München (DE)

(54) METHOD AND SYSTEM FOR DATA RECORDING / REPRODUCING, APPARATUS FOR RECORDING/REPRODUCING, AND MEDIA FOR RECORDING PROGRAM

(57) A data recording/reproducing method wherein encrypted digital data obtained by subjecting digital data to first encrypting by using a contents key and encrypted contents key obtained by subjecting the contents key to second encrypting are recorded on a recording medium, the encrypted digital data and the encrypted contents key, having been recorded, are reproduced, and the encrypted digital data is decrypted by using the contents key obtained by decrypting the encrypted contents key, thereby to obtain the digital data.

Fig. 1



DISCLOSURE OF THE INVENTION

[0011] By considering the above-mentioned problems encountered in the conventional data recording/reproducing methods, as a first object, the present invention is intended to provide a data recording/reproducing method and a data recording/reproducing system, wherein, by encrypting data, only the specific object can be reproduced and the above-mentioned encrypting-related information is less likely to leak outside.

[0012] Furthermore, in addition to the above-mentioned first object, the present invention is intended to provide a data recording/reproducing method and a data recording/reproducing system capable of securely carrying out billing at the time of recording and/or reproduction.

[0013] Moreover, in addition to the above-mentioned first object, the present invention is intended to provide a data recording/reproducing system having less loss time at the time of reproduction.

[0014] Additionally, the present invention is intended to provide a recording apparatus and a reproducing apparatus, capable of recording data on a recording medium and observing limitations on an effective reproduction period and an effective number of reproductions for the data.

BRIEF DESCRIPTION OF THE DRAWINGS

[0015]

FIG. 1 is a configuration view showing the configuration of a data recording/reproducing system in accordance with a first embodiment of the present invention;

FIG. 2 is a flow chart showing the flow of data at the time when the data recording/reproducing system in accordance with the first embodiment of the present invention records data;

FIG. 3 is a flow chart showing the flow of data at the time when the data recording/reproducing system in accordance with the first embodiment of the present invention reproduces data;

FIG. 4 is a schematic view showing the recording area on a recording medium, on which-recording is carried out by using the data recording/reproducing system in accordance with the first embodiment of the present invention;

FIG. 5 is a flow chart showing the flow of a recording medium on which recording is carried out by using the data recording/reproducing system in accordance with the second embodiment of the present invention at the time of lending/borrowing;

FIG. 6 is a flow chart showing the flow of data at the time when the data recording/reproducing system in accordance with the third embodiment of the present invention records data;

FIG. 7 is a flow chart showing the flow of data at the time when the data recording/reproducing system in accordance with the third embodiment of the present invention reproduces data;

FIG. 8 is a flow chart showing the flow of data at the time when the data recording/reproducing system in accordance with the fourth embodiment of the present invention records data;

FIG. 9 is a flow chart showing the flow of data at the time when the data recording/reproducing system in accordance with the fourth embodiment of the present invention reproduces data;

FIG. 10 is a configuration view showing the configuration of a data recording/reproducing system in accordance with a fifth embodiment of the present invention;

FIG. 11 is a flow chart showing the flow of data at the time when the data recording/reproducing system in accordance with the fifth embodiment of the present invention records data;

FIG. 12 is a flow chart showing the flow of data at the time when the data recording/reproducing system in accordance with the fifth embodiment of the present invention reproduces data;

FIG. 13 is a configuration view showing the configuration of another data recording/reproducing system in accordance with the fifth embodiment of the present invention;

FIG. 14 is a flow chart showing the flow of data at the time when the other data recording/reproducing system in accordance with the fifth embodiment of the present invention records data;

FIG. 15 is a configuration view showing the configuration of a data recording/reproducing system in accordance with a sixth embodiment of the present invention;

FIG. 16 is a flow chart showing the flow of data at the time when the data recording/reproducing system in accordance with the sixth embodiment of the present invention records data;

FIG. 17 is a flow chart showing the flow of data at the time when the data recording/reproducing system in accordance with the sixth embodiment of the present invention reproduces data;

FIG. 18 is a configuration view showing the configuration of another data recording/reproducing system in accordance with the sixth embodiment of the present invention;

FIG. 19 is a flow chart showing the flow of data at the time when the other data recording/reproducing system in accordance with the sixth embodiment of the present invention records data;

FIG. 20 is a flow chart showing the flow of data at the time when the other data recording/reproducing system in accordance with the sixth embodiment of the present invention reproduces data;

FIG. 21 is a flow chart showing the flow of data at the time when a data recording/reproducing system in accordance with a seventh embodiment of the

referring to FIG. 2. FIG. 2 is a flow chart showing the flow of data at the time when the data recording/reproducing system in accordance with the first embodiment of the present invention records data. Referring to FIG. 2, in the configuration shown in FIG. 1, means not required during recording are omitted as appropriate. In addition, D represents plain data of the AV data to be recorded, Kco represents a contents key used to encrypt AV data D, Kco (D) represents encrypted AV data obtained by encrypting the AV data D by using the contents key Kco, STB Pa represents a public key inherent in the STB 1 and used for encrypting the contents key Kco, and STB Pa (Kco) represents a encrypted contents key obtained by encrypting the contents key Kco by using the public key STB Pa, respectively. Furthermore, by switching the contents key Kco at regular or irregular intervals, the data recording/reproducing system in accordance with the present embodiment becomes a system wherein encrypting-related information is less likely to leak outside than in the case when the switching is not carried out.

[0023] First, the receiving/demodulating means 21 receives digital video data, audio data, EMM (individual information), ECM (program information) and encrypted broadcasting scrambling key Ks received from a broadcasting station via the antenna 3, shapes the disturbances in the signal waveforms of the video data and the audio data, and outputs the video data, audio data, EMM, ECM and encrypted broadcasting scrambling key Ks to the DMUX 23.

[0024] The EMM (individual information) is information required to generate a key referred to as a work key Kw described later.

[0025] Furthermore, the ECM (program information) is information required to restore the encrypted broadcasting scrambling key Ks.

[0026] Then, the DMUX 23 receives the video data, audio data, EMM, ECM and broadcasting scrambling key Ks from the receiving/demodulating means 21, demultiplexes them, and outputs the video data and audio data (AV data) to the broadcasting descrambling means 20. Furthermore, the means outputs the EMM to an EMM decrypting means 25, and also outputs the ECM and the encrypted broadcasting scrambling key Ks to an ECM decrypting means 24.

[0027] Next, the EMM decrypting means 25 receives a user ID key Km, also receives the EMM from the DMUX 23, decrypts the EMM by using the user ID key Km to generate the work key Kw, and outputs it to the ECM decrypting means 24.

[0028] Furthermore, the ECM decrypting means 24 receives the work key Kw from the EMM decrypting means 25, also receives the ECM and the encrypted broadcasting scrambling key Ks from the DMUX 23, decrypts the ECM by using the work key Kw to restore the encrypting of the encrypted broadcasting scrambling key Ks, and outputs it to the broadcasting descrambling means 20.

[0029] And the broadcasting descrambling means 20 receives the broadcasting scramble key Ks from the ECM decrypting means 24 and also receives scrambled AV data from the DMUX 23, and then descrambles the scrambled AV data by using the broadcasting scrambling key Ks.

[0030] The AV data D, having been scrambled for broadcasting, is descrambled by the broadcasting descrambling means 20 and demultiplexed by the DMUX 23 to become plain AV data D, and the plain AV data D is sent to the video decoder 11, the audio decoder 12 and the contents encrypting means 13. The video decoder 11 and the audio decoder 12 decode highly efficient coding and the like applied to the AV data D, and then output data to the display 4. The contents encrypting means 13 generates a contents key Kco, and encrypts the AV data D by using the generated contents key Kco to generate encrypted AV data Kco (D). The generated contents key Kco is sent to the key encrypting means 15, and the key encrypting means 15 encrypts the contents key Kco by using the public key STB Pa stored in the STB information storing means 17 and inherent in the STB 1 to generate the encrypted contents key STB Pa (Kco),

[0031] The encrypted AV data Kco (D) and the encrypted contents key STB Pa (Kco) are transmitted to the VTR apparatus 5 via the D-I/F 18 and via the certified key exchanging means 19 and the D-I/F 18, respectively; however, before the transmission, the certified key exchanging means 19 and 52 corresponding to the STB 1 and the VTR apparatus 5, respectively, exchange their certified keys to each other via the D-I/Fs 18 and 51 to confirm that they are parties transmittable to each other, and the above-mentioned transmission is carried out.

[0032] The encrypted AV data Kco (D) and the encrypted contents key STB Pa (Kco), transmitted to the VTR apparatus 5, are sent to the MUX 54 via the D-I/F 51 and via the D-I/F 51 and the certified key exchanging means 52, respectively; and they are multiplexed in accordance with the format of the recording medium 6, and then recorded on the recording medium 6 by the recording means 55.

[0033] Next, the flow of data at the time when the AV data recorded on the recording medium 6 is reproduced will be described below referring to FIG. 3. FIG. 3 is a flow chart showing the flow of data at the time when the data recording/reproducing system in accordance with the first embodiment of the present invention reproduces data. Referring to FIG. 3, in the configuration shown in FIG. 1, means not required during reproduction are omitted as appropriate. STB Sa corresponds to the public key STB Pa and represents a secret key inherent in the STB 1 and used to decrypt the encrypted contents key STB Pa (Kco) to restore the contents key Kco. The other reference encrypts in the figure are the same as those used in FIG. 2.

[0034] The encrypted AV data Kco (D) and the

billing information can be generated by using the above-mentioned required information at the time when the recording medium 6 is reproduced. At this time, for example, the STB control means generates the above-mentioned required information during the recording, sends this to the recording means 55 via the D-I/Fs 18 and 51, and the recording means 55 records this in the first part of data to be recorded. During the reproduction, the above-mentioned required information is reproduced by the reproducing means 58 and sent to the STB control means via the D-I/Fs 18 and 51; and on the basis of this, the STB control means generates the billing information for reproduction by using the billing information generating means 22.

[0046] From the above-mentioned descriptions, it is understood that the data recording/reproducing system of the present embodiment is a data recording/reproducing system capable of securely carrying out billing during recording and/or reproduction.

[0047] Next, the recording area on the recording medium, for data recorded on the recording medium by the data recording/reproducing system of the present embodiment, will be described below referring to FIGS. 2 and 4.

[0048] FIG. 4 is a schematic view showing the recording area on the recording medium, on which recording is carried out by using the data recording/reproducing system in accordance with the first embodiment of the present invention. The left-to-right direction of FIG. 4 indicates the recording position on the recording medium 6 with respect to time, and the up-to-down direction indicates the configuration of data recorded at the same time. Referring to FIG. 4, the recording area is divided into a main area and a sub-area. In the main area, encrypted AV data and a flag indicating the timing for changing contents key are written; and in the sub-area, at the contents keys (Kco-a, Kco-b, Kco-c, Kco-d, ...) used for encrypting the encrypted AV data (Kco-a (D), Kco-b (D), Kco-c (D), Kco-d (D), ...) recorded in the main area positions corresponding to the recording positions, encrypted contents keys (STB Pa (Kco-a), STB Pa (Kco-b), STB Pa (Kco-c), STB Pa (Kco-d), ...) obtained by encrypting by using the public key STB Pa are written; and at the contents keys (Kco-b, Kco-c, Kco-d, Kco-e, ...) for use after switching of the next contents key, encrypted contents keys (STB Pa (Kco-b), STB Pa (Kco-c), STB Pa (Kco-d), STB Pa (Kco-e), ...) obtained by encrypting by using the public key STB Pa are written. However, for purposes of convenience, in FIG. 4, the encrypted contents keys STB Pa (Kco-a), STB Pa (Kco-b), STB Pa (Kco-c), STB Pa (Kco-d), ... are represented by the contents keys Kco-a, Kco-b, Kco-c, Kco-d, ... , which are contents keys for use before encrypting.

[0049] As described above, the contents encrypting means 13 generates the contents key Kco by switching at regular or irregular intervals, and encrypts the AV data D by using the generated contents key Kco to generate the encrypted AV data Kco (D); however, the contents encrypting mean previously generates a contents key (for example, Kco-b) to be obtained by switching next to the current contents key (for example, Kco-a), and before using it, converts it into the encrypted contents key STB Pa (Kco-a) by the key encrypting means 15, and sends it to the MUX54 via the certified key exchanging means 19 and the D-I/Fs 18 and 51; and then the recording means 55 records it together with the current contents key Kco-a, the encrypted AV data Kco-a (D) encrypted thereby and the like in the recording area shown in FIG. 4. The flag indicating the timing for changing contents key is added to, for example, a packet header for transmitting AV data and then transmitted; on the basis of this, the recording means 55 determines the recording position of each piece of recording data.

[0050] As shown in FIG. 4, the encrypted contents key STB Pa (Kco-b) corresponding to a contents key for use after switching, for example, Kco-b, is recorded on the recording medium 6 so as to overlap at least a part of the encrypted AV data Kco-a (D) corresponding to the contents key Kco-a for use before switching, and the contents key Kco-a for use before switching is recorded on the recording medium 6 so as to overlap the position wherein the encrypted AV data Kco-a (D) corresponding thereto is recorded. Referring to FIG. 4, in the recording area for the encrypted contents key STB Pa (Kco-b), writing has been completed immediately before the encrypted contents key STB Pa (Kco-c) corresponding to the next contents key Kco-c is written; however, the writing should only be completed at least before the encrypted contents key STB Pa (Kco-c) is written; in other words, if recording is completed so that the recording area for the encrypted contents key STB Pa (Kco-b) in FIG. 4 overlaps at least a part of the encrypted AV data Kco-a (D), a data blank area may be present between the recording area and the starting end of the recording area for the encrypted contents key STB Pa (Kco-c).

[0051] By carrying out recording on the recording medium in accordance with the above-mentioned procedure, the next contents key can be decrypted beforehand during reproduction; therefore, it is understood that the data recording/reproducing system of the present embodiment is a data recording/reproducing system causing less loss time during reproduction.

[0052] The recording procedure for recording in the recording area on the recording medium of the present invention is not limited to the above-mentioned recording procedure of the present embodiment; for example, it may be possible to use a procedure wherein the contents encrypting means 13 does not previously generate the contents key for use after the next switching, but the VTR apparatus 5 has a means for temporarily storing data sent from the STB 1 and allows the above-mentioned temporary storing means to temporarily store the current data, and the recording area on the recording

first embodiment.

[0064] The operations of the present embodiment will be described below.

[0065] FIG. 6 is a flow chart showing the flow of data at the time when the data recording/reproducing system in accordance with the second embodiment of the present invention records data; and FIG. 7 is a flow chart showing the flow of data at the time when the data recording/reproducing system in accordance with the second embodiment of the present invention reproduces data. As shown in FIGS. 6 and 7, the configuration in accordance with the present embodiment is the same as that of the data recording/reproducing system in accordance with the first embodiment, except that a public key USER Pa inherent in the user ID recorded on the IC card 2 is used to encrypt the contents key Kco, and that a secret key USER Sa inherent in the user ID is used to decrypt the contents key Kco.

[0066] By recording/reproducing AV data in accordance with the above-mentioned procedure, in the configuration of the present embodiment, in addition to the effects obtained in accordance with the first embodiment, it is understood that even if the STB 1 cannot be used because of an unrepairable failure or breakdown, continuous use is possible by replacing it with another STB (a device model other than the same device model can be used), and furthermore that another user can use the system through lending or borrowing of the recording medium 6 together with the IC card 2.

[0067] Furthermore, in the present embodiment, provided that, in order to encrypt the contents key Kco as described above, the encrypted contents key USER Pa (Kco) is generated by using the public key USER Pa inherent in the user ID recorded on the IC card 2, and the encrypted contents key USER1 Pa (Kco) is also generated by using the public key USER1 Pa inherent in another user ID recorded on the IC card 2, and that these are recorded on the recording medium 6 together with the encrypted contents key USER Pa (Kco), a specific user having the secret key USER1 Sa corresponding to the public key USER1 Pa can restore the encrypted contents key USER1 Pa (Kco) by using the USER1 Sa; therefore, the recording medium 6 can be lent only to the specific user. The number of the public key USER1 Pa is not limited to one, but plural public keys, such as USER1 Pa to USERn Pa, may be available. In other words, the user can simply lend the medium to another user, in the case when he wishes to borrow and use it, by having the other user record the public key USERn Pa corresponding thereto on the IC card 2 in accordance with a predetermined procedure.

[0068] As understood from the above-mentioned operations, in the present embodiment, the STB storing means 11 may be omitted from the configuration of the data recording/reproducing system in accordance with the first embodiment shown in FIG. 1.

(Fourth embodiment)

[0069] A fourth embodiment in accordance with the present invention will be described below referring to the drawings. The present embodiment differs from the above-mentioned first embodiment in that the public key/secret key for encrypting/decrypting the contents key are keys inherent in the service recorded on the IC card of the present invention. For this reason, the same components as those used for the first embodiment are represented by the same reference codes, and the explanations of these components are omitted. Furthermore, components not described specifically are the same as those of the first embodiment.

[0070] The configuration of the data recording/reproducing system in accordance with the present embodiment is the same as that of the data recording/reproducing system in accordance with the first embodiment.

[0071] The operations of the present embodiment will be described below.

[0072] FIG. 8 is a flow chart showing the flow of data at the time when the data recording/reproducing system in accordance with the fourth embodiment of the present invention records data; and FIG. 9 is a flow chart showing the flow of data at the time when the data recording/reproducing system in accordance with the fourth embodiment of the present invention reproduces data. As shown in FIGS. 8 and 9, the configuration in accordance with the present embodiment is the same as that of the data recording/reproducing system in accordance with the first embodiment, except that a public key SERV Pa inherent in the service recorded on the IC card 2 is used to encrypt the contents key Kco, and that a secret key SERV Sa inherent in the device model of the STB 1 is used to restore the contents key Kco. More specifically, the key inherent in the service includes keys inherent in a specific program only, inherent in programs of a specific genre only, inherent in programs in a specific channel only, inherent in a specific satellite broadcasting provider only, and the like.

[0073] For example, by previously paying the charge for the recording/reproduction of a specific program, the public key SERV Pa and the secret key SERV Sa inherent in the program are allowed to be stored in the IC card 2, whereby the above-mentioned specific program can be recorded/reproduced. In this case, if the public key SERV Pa and the secret key SERV Sa are not stored on the IC card 2, the STB 1 is required to take a measure to prevent recording. In the case of a program other than the specific program requiring the public key SERV Pa and the secret key SERV Sa, the public key and the secret key used for one of the first to third embodiments are selected and used; these methods can be used in combination.

[0074] By recording/reproducing AV data in accordance with the above-mentioned procedure, in the configuration of the present embodiment, in addition to the

STB 1 and the VTR apparatus 5, respectively, exchange their certified keys via the D-I/Fs 18 and 51 to confirm that they are parties transmittable to each other, and the above-mentioned transmission is carried out.

[0083] The encrypted AV data Kco (D) transmitted to the VTR apparatus 5 is sent to the MUX 54 via the D-I/F 51. In addition, the encrypted contents key Kk (Kco) transmitted to the VTR apparatus 5 is sent to the key decrypting means 61 via the D-I/F 51 and the certified key exchanging means 52. The key decrypting means 61 decrypts the encrypted contents key Kk (Kco) to restore the contents key Kco by using the common key Kk stored in the VTR information storing means 71, and sends it to the key encrypting means 62. The key encrypting means 62 encrypts the contents key Kco by using the public key STB Pa inherent in the STB 1 and stored in the VTR information storing means 71 to generate the encrypted contents key STB Pa (Kco), and sends it to the MUX 54. The encrypted AV data KCo (D) and the encrypted contents key STB Pa (Kco) sent to the MUX 54 are multiplexed in accordance with the format of the recording medium 6, and then recorded on the recording medium 6 by the recording means 55.

[0084] Next, the flow of data at the time when AV data recorded on the recording medium 6 is reproduced will be described below referring to FIG. 12. FIG. 12 is a flow chart showing the flow of data at the time when the data recording/reproducing system in accordance with the fifth embodiment of the present invention reproduces data. As shown in FIG. 12, in the present embodiment, the encrypted contents key STB Pa (Kco) having been recorded is not restored in the VTR apparatus 5 but sent to the key decrypting means 16 of the STB 1, and restored herein to the contents key Kco by using the secret key STB Sa inherent in the STB 1 and stored in the STB information storing means 17. Means and the like not required for reproduction are omitted as appropriate from the configuration shown in FIG. 1. In other words, the flow of data at the time of reproducing the AV data is the same as that of the first embodiment shown in FIG. 3.

[0085] By recording/reproducing the AV data in accordance with the above-mentioned procedure, the encrypting of the contents key at the STB 1 on the transmission side to the VTR apparatus 5 is carried out during AV data recording by using the common key which causes a less burden; therefore, the burden to the STB 1 having an increased burden due to the concurrent encrypting of the AV data and the contents key can be decreased; for this reason, it is understood that the data recording/reproducing system of the present embodiment can reproduce only the specific object, thereby becoming a data recording/reproducing system wherein encrypting-related information is less likely to leak outside, and furthermore that the system is capable of having higher recording efficiency by smoothing the burden to the STB 1 and the VTR apparatus 5, in comparison with the data recording/reproducing system of the first embodiment.

[0086] In the present embodiment, it is explained that the public key and the secret key of the present invention are keys inherent in the tuner apparatus (STB 1) of the present invention, just as in the case of the first embodiment; however, without being limited to this, just as in the case of one of the second to fourth embodiments, for example, the keys may be keys inherent in the device model of the tuner apparatus (STB 1) of the present invention, inherent in the user ID recorded on the IC card of the present invention, and inherent in the service recorded on the IC card of the present invention.

[0087] Furthermore, it is explained that the public key information of the present invention is stored in the VTR information storing means 71 in the case of the present embodiment; however, without being limited to this, the information may be sent from the STB 1 at the start of recording, for example.

[0088] It is also possible to use the configuration shown in FIG. 13, wherein the key encrypting means 31 and the key decrypting means 61 are omitted from the data recording/reproducing system of the present embodiment. With this configuration, data transmission is carried out without encrypting the contents key at the time of data transmission from the tuner apparatus to the VTR apparatus of the present invention. This kind of configuration is particularly effective when applied to the data recording/reproducing system provided with an integrated STB wherein the functions of the STB and the VTR apparatus are integrated, just as in the case of an eighth embodiment described later. The data recording/reproducing system having the configuration shown in FIG. 13 will be described below.

[0089] FIG. 14 shows the flow of data at the time when AV data is recorded on the recording medium 6 in the data recording/reproducing system having the configuration shown in FIG. 13. In FIG. 14, means and the like not required for reproduction are omitted as appropriate from the configuration shown in FIG. 13. In addition, the reference encrypts in the figure are the same as those used in FIGS. 11 and 12.

[0090] The AV data D, decrypted as broadcasting radio waves and multiplexed, is received via the antenna 3, demodulated by the receiving/demodulating means 21 and decrypted by the broadcasting descrambling means 20 with respect to encrypts for broadcasting, demultiplexed by the DMUX 23 to become plain AV data D, and then sent to the video decoder 11, the audio decoder 12 and the contents encrypting means 13. The video decoder 11 and the audio decoder 12 decode highly efficient coding and the like given to the AV data D, and output data to the display 4. The contents encrypting means 13 generates contents key Kco, and encrypts the AV data D by using the generated contents key Kco, thereby to generate encrypted AV data Kco (D).

[0091] The encrypted AV data Kco (D) and the contents key Kco are transmitted to the VTR apparatus 5

ing/reproducing system in accordance with the sixth embodiment of the present invention records data. In FIG. 16, means and the like not required for recording are omitted as appropriate from the configuration shown in FIG. 15. The reference encrypts in the figure are the same as those used in FIGS. 2 and 3, except for those explained newly. Kk represents a common key that is common to the STB 1 and the VTR apparatus 5 and used to encrypt the contents key Kco, Kk (Kco) represents a encrypted contents key obtained by encrypting the contents key Kco by using the common key Kk, VTR Pa represents a public key inherent in the VTR apparatus 5 and used to encrypt the contents key Kco, and VTR Pa (Kco) represents a encrypted contents key obtained by encrypting the contents key Kco by using the public key VTR Pa, respectively. Furthermore, just as in the case of the first embodiment, by switching the contents key Kco at regular or irregular intervals, the data recording/reproducing system in accordance with the present embodiment becomes a system wherein encrypting-related information is less likely to leak outside, in comparison with the case wherein the switching is not carried out.

[0101] The AV data D, decrypted as broadcasting radio waves and multiplexed, is received via the antenna 3, demodulated by the receiving/demodulating means 21 and decrypted by the broadcasting descrambling means 20 with respect to encrypts for broadcasting, demultiplexed by the DMUX 23 to become plain AV data D, and then sent to the video decoder 11, the audio decoder 12 and the contents encrypting means 13. The video decoder 11 and the audio decoder 12 decode highly efficient coding and the like given to the AV data D, and output data to the display 4. The contents encrypting means 13 generates the contents key Kco, encrypts the AV data D by using the generated contents key Kco to generate encrypted AV data Kco (D). The generated contents key Kco is sent to the key encrypting means 31, and the key encrypting means 31 encrypts the contents key Kco by using the common key Kk common to the STB 1 and the VTR apparatus 5 and stored in the STB information storing means 17 to generate the encrypted contents key Kk (Kco).

[0102] The encrypted AV data Kco (D) and the encrypted contents key STB Pa (Kco) are transmitted to the VTR apparatus 5 via the D-I/F 18 and via the certified key exchanging means 19 and the D-I/F 18, respectively; however, before the transmission, the certified key exchanging means 19 and 52 corresponding to the STB 1 and the VTR apparatus 5, respectively, exchange their certified keys via the D-I/Fs 18 and 51 to confirm that they are parties transmittable to each other, and the above-mentioned transmission is carried out.

[0103] The encrypted AV data Kco (D) transmitted to the VTR apparatus 5 is sent to the MUX 54 via the D-I/F 51. In addition, the encrypted contents key Kk (Kco) transmitted to the VTR apparatus 5 is sent to the key decrypting means 61 via the D-I/F 51 and the certified key exchanging means 52. The key decrypting means 61 decrypts the encrypted contents key Kk (Kco) to restore the contents key Kco by using the common key Kk stored in the VTR information storing means 71 and sends it to the key encrypting means 62. The key encrypting means 62 encrypts the contents key Kco by using the public key VTR Pa inherent in the VTR apparatus 5 and stored in the VTR information storing means 71 to generate the encrypted contents key VTR Pa (Kco) and sends it to the MUX 54. The encrypted AV data Kco (D) and the encrypted contents key VTR Pa (Kco) sent to the MUX 54 are multiplexed in accordance with the format of the recording medium 6, and then recorded on the recording medium 6 by the recording means 55.

[0104] Next, the flow of data at the time when AV data recorded on the recording medium 6 is reproduced will be described below referring to FIG. 17. FIG. 17 is a flow chart showing the flow of data at the time when the data recording/reproducing system in accordance with the sixth embodiment of the present invention reproduces data. In FIG. 17, means and the like not required for reproduction are omitted as appropriate from the configuration shown in FIG. 15. VTR Sa corresponds to the public key VTR Pa, and represents a secret key inherent in the VTR apparatus 5 and used to decrypt the encrypted contents key VTR Pa (Kco) to restore the contents key Kco. The other reference encrypts in the figure are the same as those used in FIG. 16.

[0105] The encrypted AV data Kco (D) and the encrypted contents key VTR Pa (Kco), multiplexed and recorded on the recording medium 6, are reproduced by the reproducing means 58, and demultiplexed by the DMUX 57. The demultiplexed encrypted contents key VTR Pa (Kco) is sent to the key decrypting means 64. The key decrypting means 64 decrypts the encrypted contents key VTR Pa (Kw) to restore the contents key Kco by using the secret key VTR Sa inherent in the VTR apparatus 5 and stored in the VTR information storing means 71, and sends it to the key encrypting means 63. The key encrypting means 63 encrypts the contents key Kco by using the common key Kk stored in the VTR information storing means 71 to generate the encrypted contents key Kk (Kco).

[0106] The demultiplexed encrypted AV data Kco (D) and the generated encrypted contents key Kk (Kco) are transmitted to the STB 1 via the D-I/F 51 and via the certified key exchanging means 52 and the D-I/F 51, respectively; however, before the transmission, the certified key exchanging means 19 and 52 corresponding to the STB 1 and the VTR apparatus 5, respectively, exchange their certified keys via the D-I/Fs 18 and 51 to confirm that they are parties transmittable to each other, and the above-mentioned transmission is carried out just as in the case of recording.

[0107] The encrypted AV data Kco (D) transmitted to the STB 1 is sent to the contents decrypting means 14 via the D-I/F 18, and the encrypted contents key Kk

above-mentioned transmission is carried out just as in the case of recording.

[0117] The encrypted AV data Kco (D) transmitted to the STB 1 is sent to the contents decrypting means 14 via the D-I/F 18, and the contents key Kco is sent to the contents decrypting means 14 via the D-I/F 18 and the certified key exchanging means 19, respectively. The contents decrypting means 14 outputs the AV data D obtained by decrypting the encrypted AV data Kco (D) by using the contents key Kco to the video decoder 11 and the audio decoder 12. The video decoder 11 and the audio decoder 12 decode highly efficient coding and the like given to the AV data D, and output data to the display 4.

[0118] The STB information storing means 17 and the VTR information storing means 71 are not required to hold the information of the common key held in the configuration shown in FIG. 15

[0119] By recording/reproducing the AV data in accordance with the above-mentioned procedure, the data transmission between the STB 1 and the VTR apparatus 5 can be carried out without encrypting the contents key; therefore, the burden to the STB 1 and the VTR apparatus 5 during recording/reproduction can be further decreased; for this reason, it is understood that the data recording/reproducing system having the configuration shown in FIG. 18 is capable of having higher recording efficiency in comparison with the data recording/reproducing system having the configuration shown in FIG. 15. However, in comparison with the data recording/reproducing system having the configuration shown in FIG. 15, the present system is low in security for data transmission between the STB 1 and the VTR apparatus 5. This kind of configuration is particularly effective when applied to the data recording/reproducing system provided with an integrated STB wherein the functions of the STB and the VTR apparatus are integrated, just as in the case of an eighth embodiment described later.

(Seventh embodiment)

[0120] A seventh embodiment in accordance with the present invention will be described below referring to the drawings. The present embodiment differs from the above-mentioned first embodiment in that the contents key is encrypted/decrypted by using a common key instead of using the public key and the secret key. For this reason, the same components as those used for the first embodiment are designated by the same reference codes, and the explanations of these components are omitted. Furthermore, components not described specifically are the same as those of the first embodiment.

[0121] The configuration of the data recording/reproducing system in accordance with the present embodiment is the same as the configuration of the data recording/reproducing system in accordance with the first embodiment.

[0122] The operations of the present embodiment will be described below.

[0123] FIG. 21 is a flow chart showing the flow of data at the time when the data recording/reproducing system in accordance with the seventh embodiment of the present invention records data. FIG. 22 is a flow chart showing the flow of data at the time when the data recording/reproducing system in accordance with the seventh embodiment of the present invention reproduces data. As shown in FIGS. 21 and 22, the present embodiment is the same as the data recording/reproducing system of the first embodiment except that the common key Kk stored in the STB information storing means 17 is used to encrypt and decrypt the contents key Kco. The common key Kk is a key inherent in the STB 1, the device model of the STB 1, user ID or service, for example. In addition, the common key Kk may be recorded on the IC card 2. When the common key Kk is not recorded on the IC card 2, and when billing information is recorded in the STB information storing means 17 for example, the card reading means 10 may be omitted. Furthermore, when the common key Kk is not recorded in the STB storing means 11, the STB storing means 11 may be omitted.

[0124] By recording/reproducing the AV data in accordance with the above-mentioned procedure, the public key is not used to encrypt the contents key; for this reason, it is understood that the data recording/reproducing system of the present embodiment is capable of having a shorter key data length in comparison with the data recording/reproducing system of the first embodiment, thereby being capable of attaining higher recording efficiency and smaller apparatus size.

(Eighth embodiment)

[0125] An eighth embodiment in accordance with the present invention will be described below referring to the drawings. The present embodiment differs from the above-mentioned first embodiment in that, although the data recording/reproducing system of the first embodiment is provided with the tuner apparatus and the VTR apparatus of the present invention, the data recording/reproducing system of the present embodiment is provided with an apparatus having integrated functions of the above-mentioned tuner apparatus and the above-mentioned VTR apparatus. For this reason, the same components as those used for the first embodiment are represented by the same reference codes, and the explanations of these components are omitted. Furthermore, components not described specifically are the same as those of the first embodiment.

[0126] FIG. 23 is a configuration view showing the configuration of the data recording/reproducing system in accordance with the eighth embodiment of the present invention. The configuration of the data recording/reproducing system in accordance with the present embodiment differs from the configuration of the data

present invention is switched at regular or irregular intervals; if the same contents key is used, the encrypting-related information is more likely to leak outside than the case of the switching at regular or irregular intervals; however, it is still possible to say that the system is a system wherein the encrypting-related information is less likely to leak, in comparison with the conventional data recording/reproducing system.

[0138] Moreover, it is explained that, in the above-mentioned first to eighth embodiments, the second encrypting in accordance with the present invention is carried out by using the keys (the public key and the common key) different from the contents key used for the first encrypting in accordance with the present invention; however, without being limited to this, the second encrypting may be applied to the contents key itself by using the same algorithm as that corresponding to the contents key used for the first encrypting. In addition, the first encrypting may be carried out for digital data by using the common key as the contents key, and the second encrypting may be carried out by using the same common key as the above-mentioned common key, for example. Besides, the data recording/reproducing system of the present invention is mainly explained in the descriptions of the first to eighth embodiments, and the data recording/reproducing methods of the present invention correspond to the methods explained in the above-mentioned descriptions.

(Ninth embodiment)

[0139] First, the configurations of a recording apparatus and a reproducing apparatus in accordance with a ninth embodiment of the present invention will be described.

[0140] FIG. 26 is a block diagram showing the recording apparatus and the reproducing apparatus in accordance with the ninth embodiment of the present invention. The recording apparatus in accordance with the ninth embodiment of the present invention comprises a first key generating means 80, a contents encrypting means 13, a second key generating means 81, a KxFIFO 85, a key encrypting means 70, a relationship information generating means 84 and an MUX 54. Furthermore, the reproducing apparatus in accordance with the ninth embodiment of the present invention comprises a DMUX 57, a key-encrypting key obtaining means 82, a Kx latch means 86, a key decrypting means 71 and a contents decrypting means 14. Furthermore, in FIG. 26, a receiving/demodulating means 21, a DMUX 23, an EMM decrypting means 25, an ECM decrypting means 24, a broadcasting descrambling means 20, a video decoder 11 and an audio decoder 12 are also shown. Moreover, a recording medium 6 used as a recording medium and a display 4 for showing images and outputting sound are also shown.

[0141] The receiving/demodulating means 21 is a means wherein digital video data and audio data, EMM (individual information), ECM (program information) and encrypted broadcasting scrambling key Ks are input from a broadcasting station via a communications satellite, and all or parts of the signal waveforms of these are shaped.

[0142] The DMUX 23 is a means wherein the video data, audio data, EMM, ECM and encrypted broadcasting scrambling key Ks, which have been input from the receiving/demodulating means 21 and waveform-shaped are demultiplexed, and the descrambled video data and audio data having been input from the broadcasting descrambling means 20 are also demultiplexed. Furthermore, the DMUX 23 is also a means wherein the video data and audio data having been input from the contents decrypting means 14 is demultiplexed.

[0143] The EMM decrypting means 25 is a means wherein the user ID key Km is input, the EMM is input from the DMUX 23, and the EMM is decrypted by using the user ID key Km to generate the work key Kw.

[0144] The ECM decrypting means 24 is a means wherein the work key Kw is input from the EMM decrypting means 25, the ECM and the encrypted broadcasting scrambling key Ks are input from the DMUX 23, and the ECM is decrypted by using the work key Kw to restore the broadcasting scrambling key Ks.

[0145] The broadcasting descrambling means 20 is a means wherein the broadcasting scrambling key Ks is input from the ECM decrypting means 24, the scrambled AV data is input from the DMUX 23, and the scrambled AV data is descrambled by using the broadcasting scrambling key Ks.

[0146] The first key generating means 80 is a means wherein the contents key Kco for encrypting again the AV data descrambled by the broadcasting descrambling means 20 is generated.

[0147] The contents encrypting means 13 is a means wherein the AV data is input from the broadcasting descrambling means 20, the contents key Kco is input from the first key generating means 80, and the AV data D is encrypted by using the contents key Kco. In the following descriptions, the AV data D encrypted by using the contents key Kco is referred to as Kco (D).

[0148] The second key generating means 81 is a means wherein a key-encrypting key Kx for encrypting the contents key Kco generated by the first key generating means 80 is generated. It is supposed that the second key generating means 81 generates different key-encrypting keys Kx, on every day, and that these different keys Kx are referred to as Kx1, Kx2, Kx3, ..., respectively. Furthermore, it is supposed that the key-encrypting keys Kx1, Kx2, Kx3, ... are each discarded in a week.

[0149] The KxFIFO 85 is a means wherein the key-encrypting keys Kx1, Kx2, Kx3, ... are input from the second key generating means 81 and stored, and also a means having a first-in first-out function, wherein a timer is provided, and the key-encrypting keys Kx, having passed one week after input, are discarded by using

data recorded on the recording medium 6 is not the AV data itself input from the broadcasting descrambling means 20, but data subjected to contents encrypting again.

[0167] First, the case when the broadcasting descrambling means 20 outputs the AV data to the DMUX 23 is explained.

[0168] In this case, the DMUX 23 receives the AV data from the broadcasting descrambling means 20, demultiplexes it to the video data and the audio data, outputs the video data to the video decoder 11, and outputs the audio data to the audio decoder 12. Then, the video decoder 11 and the audio decoder 12 decode the video data and the audio data input from the DMUX 23, respectively, and outputs data to the display 4. And the display 4 shows images and outputs sound.

[0169] Next, the case when the broadcasting descrambling means 20 outputs the AV data to the contents encrypting means 13 is explained. In other words, this is the case when the AV data is recorded on the recording medium 6 as described above.

[0170] First, the contents encrypting means 13 receives the descrambled AV data D from the broadcasting descrambling means 20.

[0171] The first key generating means 80 generates the contents key Kco for encrypting the AV data D input from the contents encrypting means 13, and outputs it to the contents encrypting means 13 and the key encrypting means 70.

[0172] Next, the contents encrypting means 13 receives the contents key Kco from the first key generating means 80, and encrypts the AV data D by using the contents key Kco. In other words, the Kco (D) is generated. Then, the Kco (D) is output to the relationship information generating means 84 and the MUX 54.

[0173] On the other hand, the second key generating means 81 generates the key-encrypting key Kx for encrypting the contents key Kco generated by the first key generating means 80. It is supposed that the key-encrypting key Kx generated by the second key generating means 81 differs day by day. For convenience in explanation, it is hereafter supposed that the starting date of the operation of the recording apparatus is January 1, 1998, and the current date when recording is carried out is January 4, 1998, three days after the starting date, and that as shown in the key-encrypting key Kx list of Fig. 27(a), the key-encrypting key Kx generated on January 1 is Kx1, the key-encrypting key Kx generated on January 2 is Kx2, ..., and the key-encrypting key Kx generated on January 4 is Kx4. Furthermore, it is supposed that the key-encrypting key Kx is generated hereinafter in the same way. Besides, the operations of the recording apparatus on January 4 will be described hereinafter, unless otherwise specified.

[0174] As shown in the list of FIG. 27 (a), from the second key generating means 81, the KxFIFO 85 has already received and stored the key-encrypting keys Kx, one on every day, starting from January 1, the KxFIFO 85 thus has stored the key-encrypting keys, Kx1, Kx2 and Kx3 until January 3, and the KxFIFO 85 then receives and stores Kx4 on the current date, January 4. The storage is carried out so that the newest key-encrypting key Kx is placed at the top of the list of FIG. 27 (a) at all times, and older ones are ranked lower in sequence. The KxFIFO 85 discards the stored key-encrypting keys Kx1, Kx2, ..., one week after the storage of each key. For example, as shown in the list of FIG. 27 (b), the key-encrypting keys Kx1 and Kx2 are discarded on January 9, and the KxFIFO 85 stores seven key-encrypting keys in the order of Kx9, Kx8, ..., Kx4 and Kx3. In other words, the number of the key-encrypting keys Kx stored in the KxFIFO 85 remains seven.

[0175] Next, the key encrypting means 70 receives the contents key Kco from the first key generating means 80, also receives the key-encrypting key Kx4 generated on January 4, the date of recording, from the second key generating means 81 via the KxFIFO 85, and encrypts the contents key Kco by using the key-encrypting key Kx4. In other words, Kx4 (Kco) is generated.

[0176] And the relationship information generating means 84 receives the encrypted AV data Kco (D) from the contents encrypting means 13 and the Kx4 (Kco) from the key encrypting means 70, and generates information indicating a date/time when the key-encrypting key Kx4 is generated as information for establishing the relationship between the key-encrypting key Kx4 and the AV data Kco (D) encrypted by using the contents key Kco encrypted by using the key-encrypting key Kx4. In other words, date/time information, January 4, is generated.

[0177] Hereafter, the MUX 54 receives the encrypted AV data Kco (D) from the contents encrypting means 13, the Kx4 (Kco) from the key encrypting means 70 and the date/time information, i.e., January 4, from the relationship information generating means 84, and then records them as one group.

[0178] In this way, Kxn (Kco) corresponding to the key-encrypting key Kxn (n = 1, 2, ...) generated on every day, i.e., on each day, the encrypted AV data Kco (D) and the date/time information regarding the day are recorded as one group on the recording medium 6.

[0179] Next the operations of the reproducing apparatus in accordance with the ninth embodiment of the present invention will be described below.

[0180] In other words, the case of reproducing the encrypted AV data Kco (D) recorded on the recording medium 6 by the recording apparatus will be described.

[0181] For convenience in the following explanation, it is supposed that the date when the reproducing apparatus reproduces the encrypted AV data Kco (D) on the recording medium 6 is January 9. Furthermore, it is supposed that the reproducing apparatus reproduces the encrypted AV data Kco (D) recorded on the recording medium 6 on January 1 and the encrypted AV data Kco (D) recorded on the recording medium 6 on January 3.

the key encrypting means 70 corresponds to the key encrypting means thereof, the relationship information generating means 84 corresponds to the relationship information generating means thereof, and the MUX 54 corresponds to the recording means thereof, respectively. Furthermore, the key-encrypting key obtaining means 82 corresponds to the key-encrypting key obtaining means of claim 50 of the present invention, the key decrypting means 71 corresponds to the key decrypting means thereof, and the contents decrypting means 14 corresponds to the contents decrypting means thereof, respectively.

[0195] Furthermore, in the above-mentioned ninth embodiment, the first key generating means 80 generates the contents key Kco for encrypting the AV data D input by the contents encrypting means 13. However, it may be possible that the recording apparatus of the present invention is not provided with the first key generating means 80 as shown in FIG. 29, that the contents encrypting means 13 receives the broadcasting scrambling key Ks sent from a broadcasting station via the broadcasting descrambling means 20, and that the AV data D is encrypted by using the broadcasting scrambling key Ks or a key obtained by processing the broadcasting scrambling key Ks. In this case, the key encrypting means 70 receives the broadcasting scrambling key Ks or the key obtained by processing the broadcasting scrambling key Ks from the contents encrypting means 13, and decrypts it by using the key-encrypting key Kx.

[0196] Furthermore, in the above-mentioned ninth embodiment, the AV data D is encrypted by using the contents key Kco from the first key generating means 80. However, it may be possible that the recording apparatus of the present invention is not provided with the first key generating means 80 or the key encrypting means 15 as shown in FIG. 30, that the contents encrypting means 13 receives the key-encrypting key Kx from the second key generating means 81 via the KxFIFO 85, that the key-encrypting key Kx is used as the contents key Kx, and that the AV data D is encrypted by using the contents key Kx. In this case, the AV data D encrypted by using the contents key Kx, i.e., Kx (AV data) and the contents key Kx, are recorded on the recording medium 6. Moreover, in this case, the reproducing apparatus of the present invention is not provided with the key restoring means 16 as shown in FIG. 30. Accordingly, in the case of reproducing Kx (AV data), the contents-key obtaining means 83 specifies the contents key Kx corresponding thereto, and obtains it from the KxFIFO 85. Then, the contents decrypting means 14 receives Kx (AV data) from the recording medium 6 via the DMUX 57, also receives the contents key Kx from the key-encrypting key obtaining means 82 via the Kx latch means 86, and decrypts the Kx (AV data) by using the contents key Kx. For this reason, in this case, that is, the second key generating means 81 corresponds to the contents-key generating means of claims 53 and 20 of the present invention, the KxFIFO 85 corresponds to the storing means thereof, the contents encrypting means 13 corresponds to the contents encrypting means thereof, the relationship information generating means 84 corresponds to the relationship information generating means thereof, and the DMUX 23 corresponds to the recording means thereof. In addition, the contents-key obtaining means 83 corresponds to the contents-key obtaining means in claims 57 and 22 of the present invention, and the contents decrypting means 14 corresponds to the contents decrypting means thereof, respectively.

[0197] Furthermore, as shown in Fig. 31, it may be possible that the recording apparatus of the above-mentioned ninth embodiment is provided with a billing means 88, that in the case when the encrypted AV data Kco (D) is recorded on the recording medium 6, and when a predetermined amount of billing for the recording has been charged to the user, that is, only when a predetermined fee has been paid in advance by the user to a broadcasting station or the like, or only when the predetermined fee has been paid at least at the time of recording, the encrypted AV data Kco (D) can be recorded on the recording medium 6. Moreover, the billing means 88 may not be disposed at the position shown in FIG. 31, but may be disposed between the key encrypting means 15 and the MUX 54. Briefly speaking, when the encrypted AV data Kco (D) is recorded on the recording medium 6, the billing means 88 should only charge the predetermined amount of billing for the recording, and may be disposed at any place.

[0198] Furthermore, in the above-mentioned ninth embodiment, each key-encrypting key Kx is discarded after a lapse of one week; however, the date/time to be discarded is not limited to one week after generation, but may be one day or three days or 12 hours after generation. In short, each key-encrypting key Kx should only be discarded after a lapse of a predetermined period after generation.

[0199] Furthermore, in the above-mentioned ninth embodiment, the second key generating means 81 generates different key-encrypting keys Kx, one on every day; however, the second key generating means 81 may generate different key-encrypting keys Kx, one in every several hours on the same day. Moreover, the key-encrypting key Kx may be generated each time the encrypted AV data Kco (D) of a predetermined program is recorded on the recording medium 6. In other words, the key-encrypting key Kx may be generated each time when recording is started and finished. In short, the second key generating means 81 should only generate the key-encrypting key Kx for encrypting the contents key Kco of the encrypted AV data Kco to be recorded.

[0200] Furthermore, in the above-mentioned ninth embodiment, the information of the date/time when the key-encrypting key Kx is generated is used as the relationship information of the present invention; however, the relationship information of the present invention may

encrypted digital data and said encrypted contents key from said recording medium, a key decrypting means for decrypting said encrypted contents key to restore said contents key, and a contents decrypting means for decrypting said encrypted digital data by using said contents key to obtain said digital data.

5. A data recording/reproducing system in accordance with claim 4, wherein all of said means are provided for an integrated apparatus.

6. A data recording/reproducing system in accordance with claim 4, wherein said receiving means, said contents encrypting means and said contents decrypting means are provided for a tuner apparatus, and said recording means and said reproducing means are provided for a VTR apparatus.

7. A data recording/reproducing system in accordance with claim 6, wherein said second encrypting is carried out by using a public key, and said encrypted contents key is decrypted by using a secret key corresponding to said public key.

8. A data recording/reproducing system in accordance with claim 7, wherein said key decrypting means is provided for said tuner apparatus.

9. A data recording/reproducing system in accordance with claim 8, wherein said public key and said secret key are keys inherent in said tuner apparatus.

10. A data recording/reproducing system in accordance with claim 8, wherein said public key and said secret key are keys inherent in the device model of said tuner apparatus.

11. A data recording/reproducing system in accordance with claim 8, wherein said tuner apparatus has a card reading means capable of reading information recorded on an IC card.

12. A data recording/reproducing system in accordance with claim 11, wherein said public key and said secret key are keys inherent in the user ID recorded on said IC card.

13. A data recording/reproducing system in accordance with claim 11, wherein said public key and said secret key are keys inherent in the service recorded on said IC card.

14. A data recording/reproducing system in accordance with claim 12, wherein in addition to said key inherent in said user ID, a public key inherent in at least another user ID is recorded on said IC card, said key encrypting means encrypts said contents key by using said public key inherent in said other user ID, in addition to said second encrypting, thereby to generate another encrypted contents key for each public key inherent in said other user ID, and said recording means records said other encrypted contents key, in addition to said encrypted contents key.

15. A data recording/reproducing system in accordance with one of claims 8 to 14, wherein said key encrypting means is provided for said tuner apparatus or said VTR apparatus.

16. A data recording/reproducing system in accordance with claim 15, wherein, in the case when said key encrypting means is provided for said VTR apparatus, said tuner apparatus has a second key encrypting means for encrypting said contents key by using a common key, and said VTR apparatus has a second key decrypting means for decrypting said contents key encrypted by using said common key.

17. A data recording/reproducing system in accordance with claim 7, wherein said public key and said secret key are keys inherent in said VTR apparatus, and said key encrypting means and said key decrypting means are provided for said VTR apparatus.

18. A data recording/reproducing system in accordance with claim 17, wherein said tuner apparatus has a second key encrypting means for encrypting said contents key by using a common key and a second key decrypting means for decrypting said contents key encrypted by using said common key, said VTR apparatus has a third key encrypting means for encrypting said contents key by using said common key and a third key decrypting means tot decrypting said contents key encrypted by using said common key, said third key decrypting means decrypts said contents key encrypted by said second key encrypting means, and said second key decrypting means decrypts said contents key encrypted by said third second key encrypting means.

19. A data recording/reproducing system in accordance with claim 6, wherein said second encrypting and said decrypting of said encrypted contents key are executed by using a common key, and said key encrypting means and said key decrypting means are provided for said tuner apparatus.

20. A data recording/reproducing system in accordance with claim 19, wherein said common key is inherent in said tuner apparatus or the device

ital data and a contents key for encrypting said digital data and for subjecting said digital data to first encrypting by using said contents key to generate encrypted digital data,

a key-encrypting key generating means for generating a key-encrypting key for subjecting said contents key to second encrypting,

a storing means for storing said key-encrypting key and for deleting said key-encrypting key hereafter if said key-encrypting key satisfies a predetermined condition,

a key encrypting means for generating a encrypted contents key by subjecting said contents key to said second encrypting by using said key-encrypting key,

a relationship information generating means for generating the relationship information between said encrypted digital data encrypted by using said contents key and said key-encrypting key obtained by encrypting said contents key, and

a recording means for receiving said encrypted digital data, said encrypted contents key and all or part of said relationship information and for recording them on a predetermined recording medium.

40. A recording apparatus in accordance with claim 39, wherein said predetermined condition is that more than a predetermined time has passed after said key-encrypting key was stored.

41. A recording apparatus in accordance with claim 39 or 40, wherein said relationship information is information related by a date/time when said contents encrypting means receives said digital data, a date/time when said contents encrypting means encrypts said digital data by using said contents key, a date/time when said key-encrypting key generating means generates said key-encrypting key, a date/time when said storing means stores said key-encrypting key, a date/time when said key encrypting means encrypts said contents key by using said key-encrypting key, or a date/time when said recording means records said encrypted digital data on said predetermined recording medium.

42. A recording apparatus in accordance with claim 39, wherein said predetermined condition is that the number of times said key-encrypting key is used at the time of reproducing said encrypted digital data exceeds a predetermined number of times.

43. A recording apparatus in accordance with one of claims 39 to 42, wherein a contents key generating means for generating said contents key is provided, and said contents encrypting means receives said contents key from said contents key generating means.

44. A recording apparatus in accordance with one of claims 39 to 42, wherein said contents encrypting means receives said contents key from a broadcasting station and uses said contents key.

45. A reproducing apparatus comprising:

a key-encrypting key obtaining means for receiving said relationship information on said recording medium of said recording apparatus in accordance with one of claims 39 to 44, for specifying a key-encrypting key corresponding to said encrypted digital data to be reproduced on the basis of said relationship information, and for retrieving and obtaining said key-encrypting key from said storing means of said recording means,

a key decrypting means for receiving said encrypted contents key corresponding to said encrypted digital data to be reproduced, from said predetermined recording medium, for receiving said key-encrypting key, and for decrypting said encrypted contents key by using said key-encrypting key, and

a contents decrypting means for decrypting said encrypted digital data by using said contents key from said key decrypting means.

46. A recording apparatus comprising:

a contents encrypting means for receiving digital data and a contents key for encrypting said digital data and for subjecting said digital data to first encrypting by using said contents key to generate encrypted digital data,

a key-encrypting key generating means for generating a key-encrypting key for subjecting said contents key to second encrypting,

a storing means for storing said key-encrypting key generated by said key-encrypting key generating means,

a key encrypting means for encrypting said contents key by using said key-encrypting key,

a relationship information generating means for generating the relationship information between said encrypted digital data encrypted by using said contents key and said key-encrypting key obtained by encrypting said contents key, and

a recording means for receiving said encrypted digital data, said encrypted contents key and all or part of said relationship information and for recording them on a predetermined recording medium.

47. A recording apparatus in accordance with claim 46,

a contents key corresponding to said encrypted digital data to be reproduced on the basis of said relationship information, and for retrieving and obtaining said contents key from said storing means of said recording means, and

a contents decrypting means for receiving said encrypted digital data from said predetermined recording medium, for receiving said contents key, and for decrypting said encrypted digital data by using said contents key.

58. A recording apparatus comprising:

a contents key generating means for generating a contents key for encrypting digital data,

a storing means for storing said contents key generated by said contents key generating means,

a contents encrypting means for encrypting said digital data by using said contents key to obtain encrypted digital data,

a relationship information generating means for generating the relationship information between said encrypted digital data encrypted by using said contents key and said contents key, and a recording means for receiving said encrypted digital data and all or part of said relationship information, and for recording them on a predetermined recording medium.

59. A recording apparatus in accordance with claim 58, wherein said relationship information is information related by a date/time when said contents encrypting means receives said digital data, a date/time when said contents encrypting means contents-encrypts said digital data by using said contents key, a date/time when said contents key generating means generates said contents key, a date/time when said storing means stores said contents key, or a date/time when said recording means records said encrypted digital data on said predetermined recording medium.

60. A reproducing apparatus comprising:

a contents-key obtaining means for receiving said relationship information on said recording medium of said recording apparatus in accordance with claim 58 or 59, for specifying a contents key corresponding to said encrypted digital data to be reproduced on the basis of said relationship information, for judging whether said contents key satisfies a predetermined condition, and for taking out said contents key from said storing means of said recording apparatus when said condition is satisfied, or for not taking out said contents key from said storing means when said condition is not satisfied, and

a contents decrypting means for decrypting said encrypted digital data by using said contents key.

61. A reproducing apparatus in accordance with claim 60, wherein said predetermined condition is that more than a predetermined time has passed after said contents key was stored in said storing means of said recording apparatus in accordance with claim 58 or 59.

62. A reproducing apparatus in accordance with claim 60, wherein said predetermined condition is that the number of times said contents key is used at the time of reproducing said encrypted digital data exceeds a predetermined number of times.

63. A recording apparatus in accordance with one of claims 39 to 44, one of claim 46 or 49, one of claim 53 or 56, or one of claims 58 to 59, provided with a billing means for charging the amount of billing for recording said data at the time when said recording means records said encrypted digital data on said predetermined recording medium.

64. A recording apparatus in accordance with one of claims 39 to 44, one of claim 46 or 49, one of claim 53 or 56, or one of claims 58 to 59, wherein said predetermined recording medium is a video tape.

65. A recording apparatus in accordance with one of claims 39 to 44, one of claim 46 or 49, one of claim 53 or 56, or one of claims 58 to 59, wherein said predetermined recording medium is a hard disk.

66. A program medium containing programs for attaining all or part of said components in accordance with one of claims 1 to 65.

Fig. 2

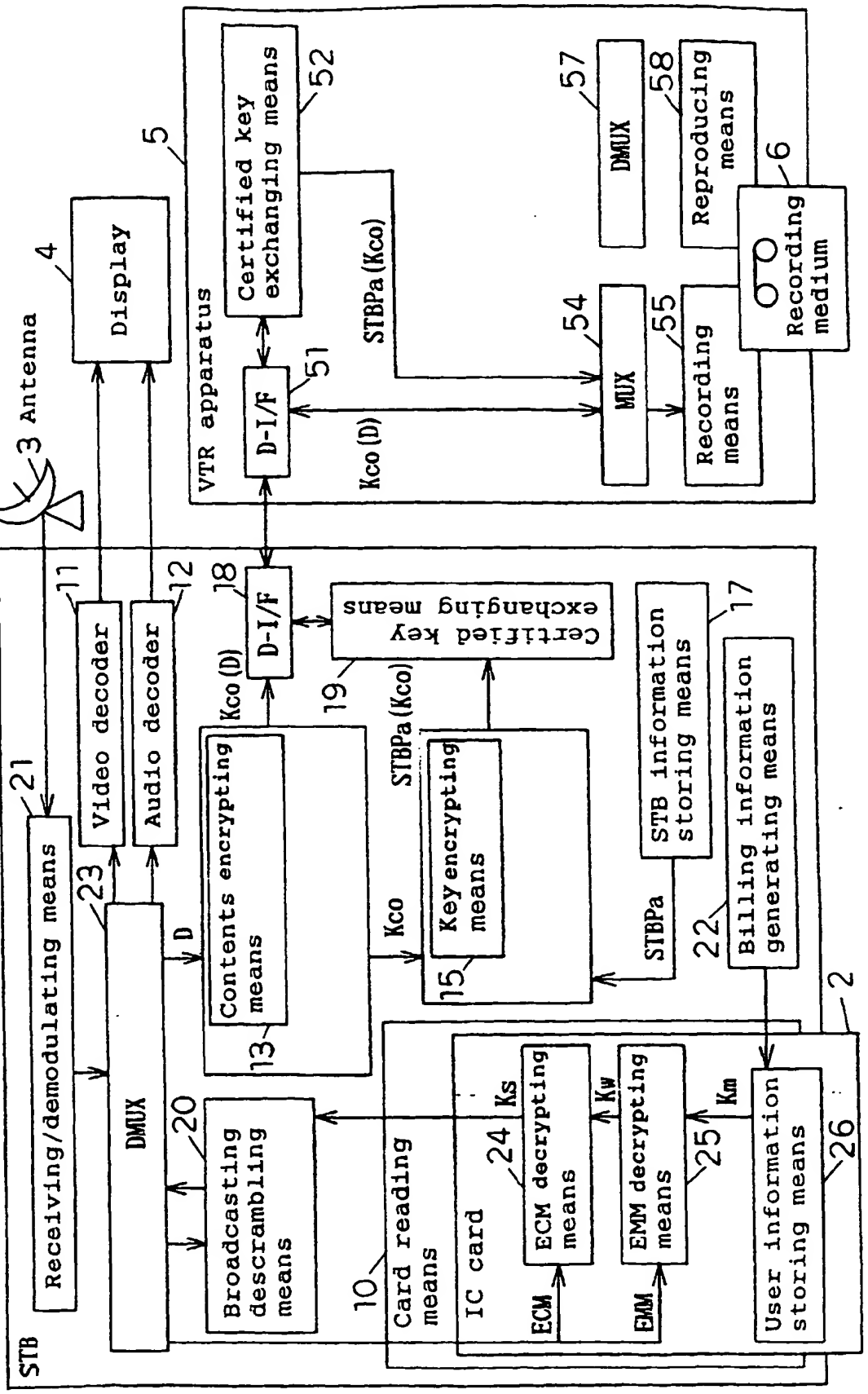

STB
1
Receiving/demodulating means
21
Video decoder
11
Audio decoder
12
DMUX
23
D
20
Broadcasting descrambling means
Card reading means
10
IC card
Ks
24
ECM decrypting means
Kw
EMM decrypting means
25
Km
User information storing means
26
2
ECM
EMM
Contents encrypting means
13
Kco (D)
D-I/F
18
Kco
Key encrypting means
15
STBPa (Kco)
Certified key exchanging means
19
STBPa
STB information storing means
17
Billing information generating means
22
3 Antenna
4
Display
5
VTR apparatus
Certified key exchanging means
52
D-I/F
51
Kco (D)
STBPa (Kco)
MUX
54
Recording means
55
DMUX
57
Reproducing means
58
Recording medium
6

Fig. 4

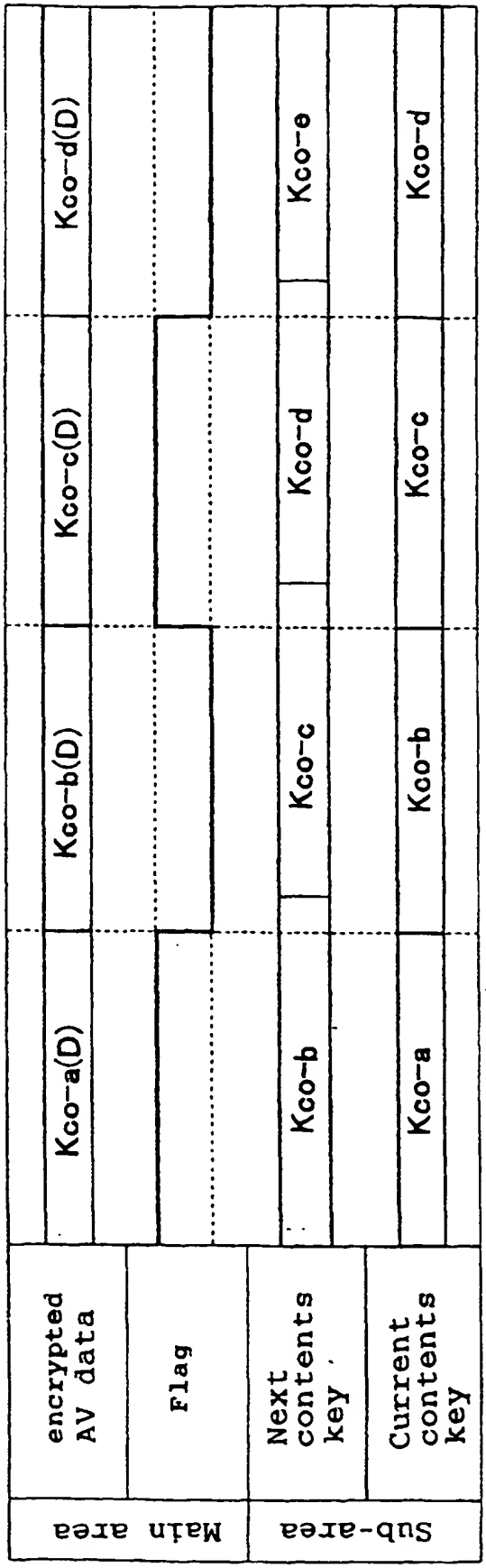

Main area
Sub-area
encrypted AV data
Flag
Next contents key
Current contents key
Kco-a(D)
Kco-b(D)
Kco-c(D)
Kco-d(D)
Kco-b
Kco-c
Kco-d
Kco-e
Kco-a
Kco-b
Kco-c
Kco-d
→ Time

Fig. 6

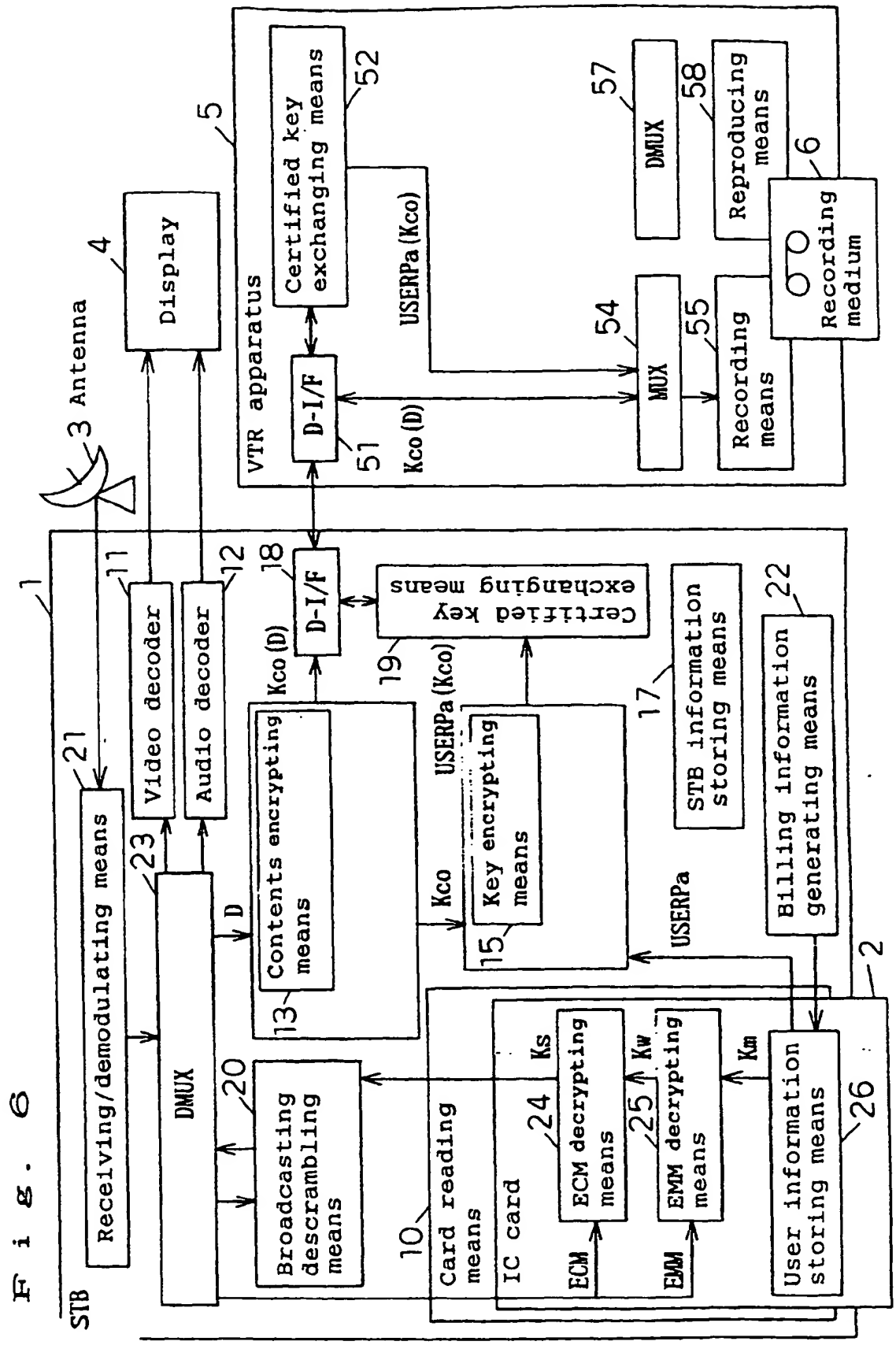

STB
1
Receiving/demodulating means
21
Video decoder
11
Audio decoder
12
DMUX
23
D
Broadcasting descrambling means
20
Card reading means
10
IC card
Ks
ECM decrypting means
24
Kw
EMM decrypting means
25
Km
ECM
EMM
User information storing means
26
2
Contents encrypting means
13
Kco (D)
D-I/F
18
Certified key exchanging means
19
USERPa (Kco)
Key encrypting means
15
Kco
USERPa
STB information storing means
17
Billing information generating means
22
3 Antenna
4
Display
5
VTR apparatus
Certified key exchanging means
52
D-I/F
51
Kco (D)
USERPa (Kco)
MUX
54
Recording means
55
DMUX
57
Reproducing means
58
Recording medium
6

Fig. 8

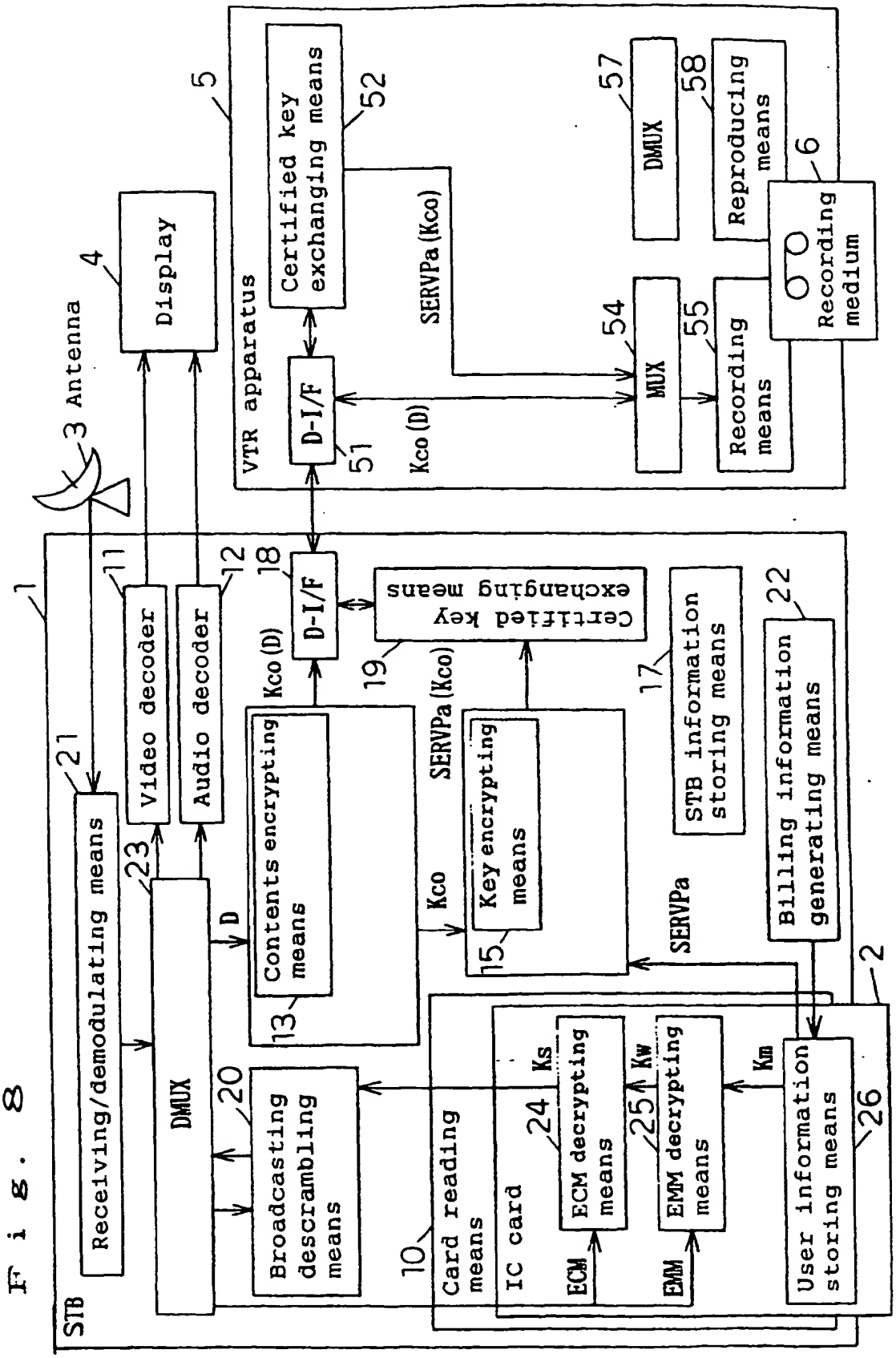

STB
1
Receiving/demodulating means
21
Video decoder
11
Audio decoder
12
DMUX
23
D
Broadcasting descrambling means
20
Contents encrypting means
13
Kco (D)
D-I/F
18
Certified key exchanging means
19
SERVPa (Kco)
Kco
Key encrypting means
15
SERVPa
STB information storing means
17
Billing information generating means
22
2
Card reading means
10
IC card
ECM
ECM decrypting means
24
Ks
EMM
EMM decrypting means
25
Kw
Km
User information storing means
26
3 Antenna
4
Display
5
VTR apparatus
Certified key exchanging means
52
D-I/F
51
Kco (D)
SERVPa (Kco)
MUX
54
Recording means
55
DMUX
57
Reproducing means
58
Recording medium
6

Fig. 10

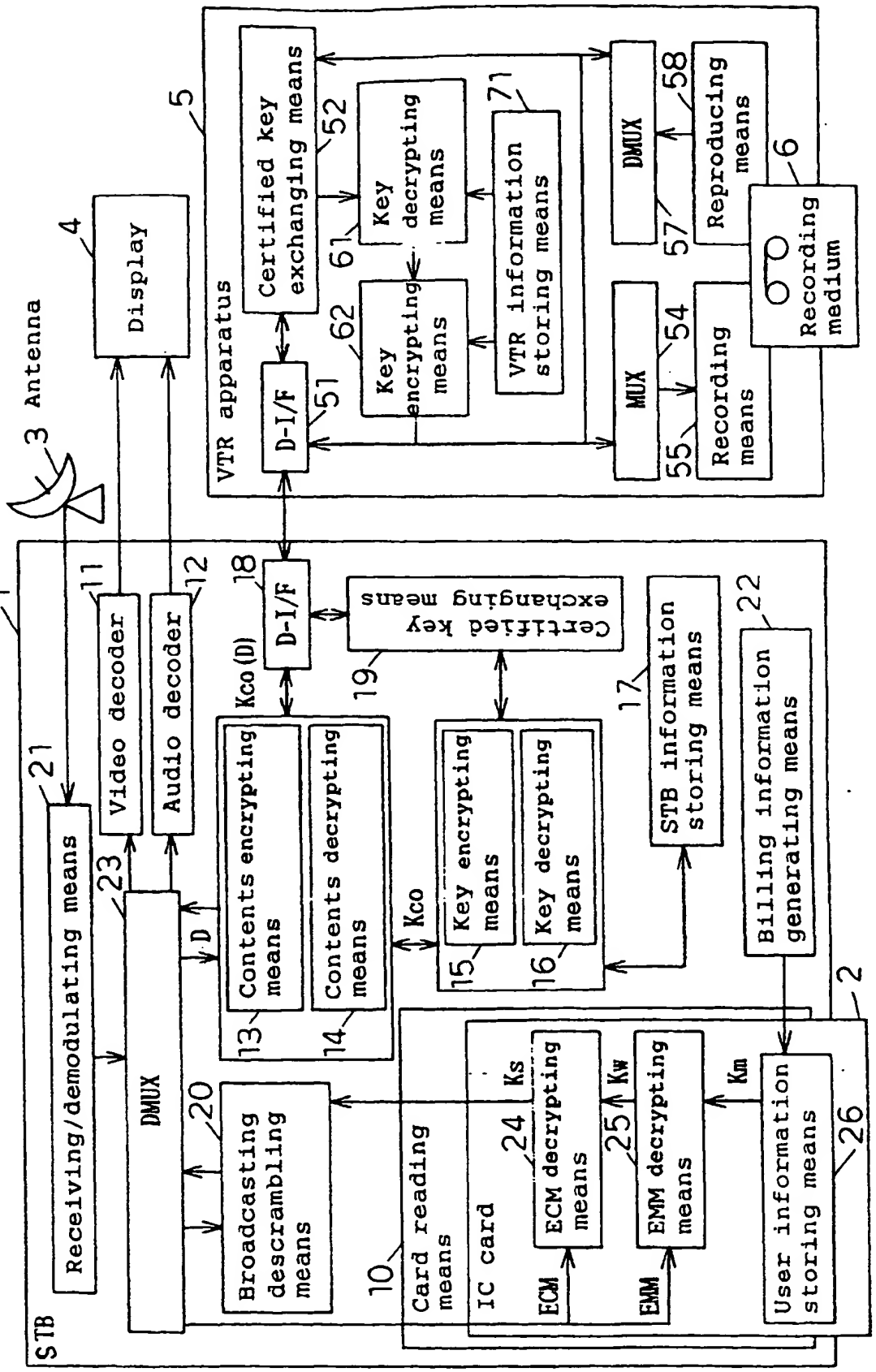

STB
1
Receiving/demodulating means
21
Video decoder
11
Audio decoder
12
DMUX
23
D
Broadcasting descrambling means
20
Card reading means
10
IC card
Ks
ECM decrypting means
24
Kw
EMM decrypting means
25
Km
ECM
EMM
User information storing means
26
2
Kco(D)
D-I/F
18
Certified key exchanging means
19
Contents encrypting means
13
Contents decrypting means
14
Kco
Key encrypting means
15
Key decrypting means
16
STB information storing means
17
Billing information generating means
22
3 Antenna
4
Display
5
VTR apparatus
D-I/F
51
Certified key exchanging means
52
Key encrypting means
62
Key decrypting means
61
VTR information storing means
71
MUX
54
Recording means
55
DMUX
57
Reproducing means
58
6
Recording medium

Fig. 12

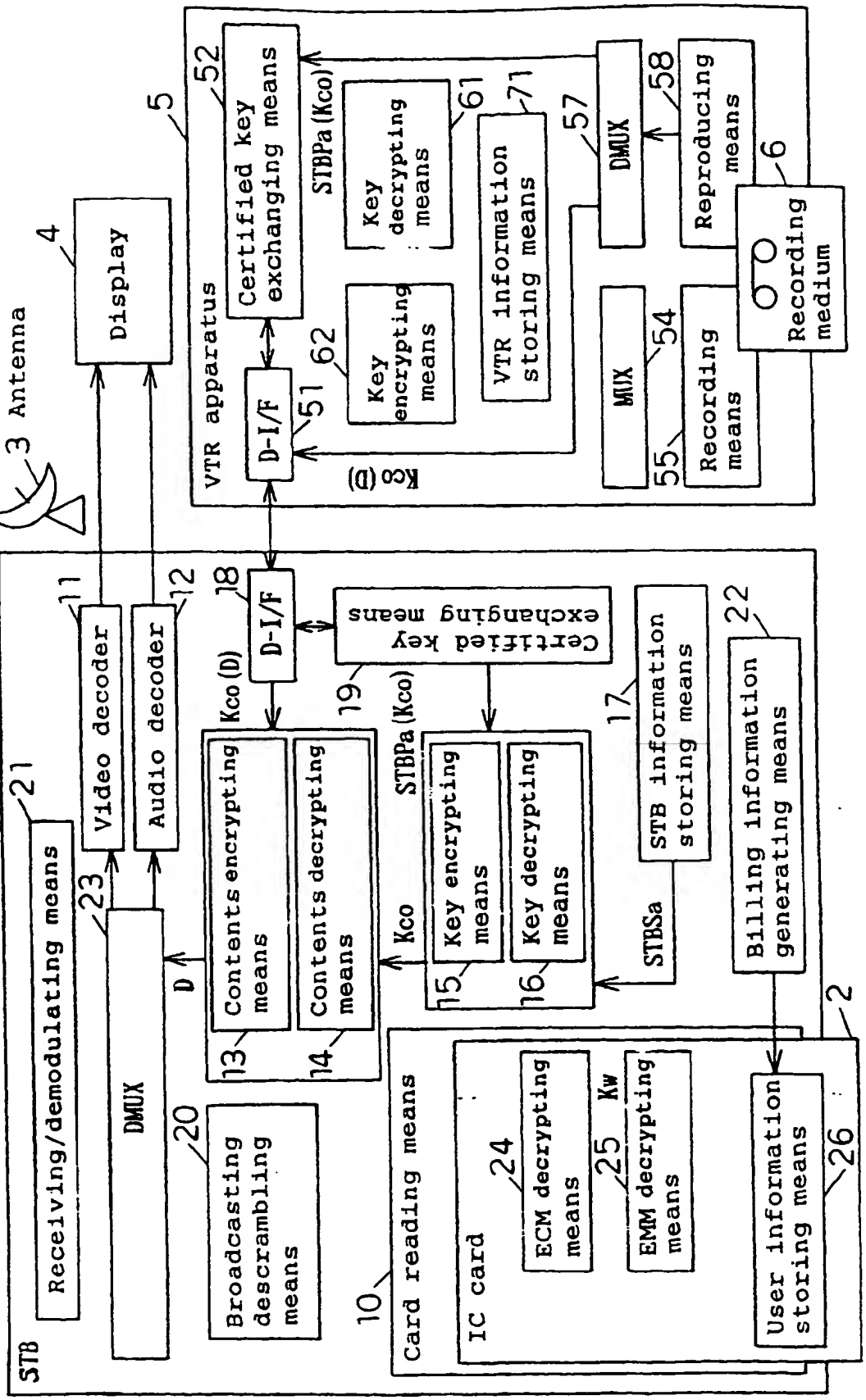

STB
1
Receiving/demodulating means
21
Video decoder
11
Audio decoder
12
DMUX
23
20
Broadcasting descrambling means
D
Kco (D)
D-I/F
18
Contents encrypting means
13
Contents decrypting means
14
Certified key exchanging means
19
Kco
STBPa (Kco)
Key encrypting means
15
Key decrypting means
16
STBSa
17
STB information storing means
22
Billing information generating means
10
Card reading means
IC card
24
ECM decrypting means
25
Kw
EMM decrypting means
User information storing means
26
2
3 Antenna
4
Display
5
VTR apparatus
52
Certified key exchanging means
STBPa (Kco)
61
Key decrypting means
71
VTR information storing means
57
DMUX
58
Reproducing means
6
Recording medium
D-I/F
51
62
Key encrypting means
Kco (D)
MUX
54
55
Recording means

Fig. 14

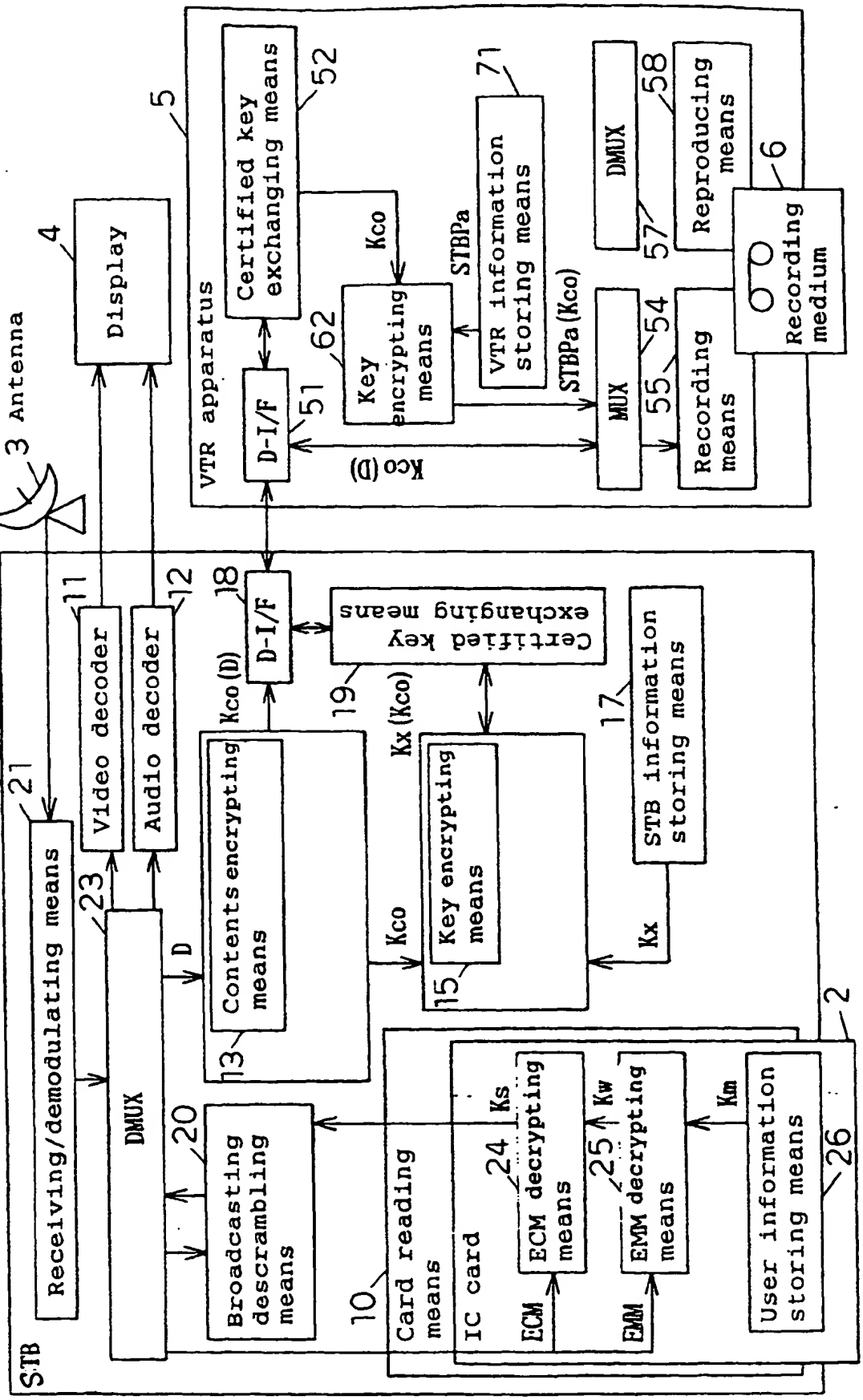

STB
1
Receiving/demodulating means
21
Video decoder
11
Audio decoder
12
DMUX
23
D
Broadcasting descrambling means
20
Card reading means
10
IC card
ECM
24
ECM decrypting means
Ks
EMM
25
EMM decrypting means
Kw
User information storing means
26
Km
2
Contents encrypting means
13
Kco (D)
D-I/F
18
Certified key exchanging means
19
Kx (Kco)
Key encrypting means
15
Kco
Kx
STB information storing means
17
3 Antenna
4
Display
5
VTR apparatus
Certified key exchanging means
52
D-I/F
51
Kco (D)
Key encrypting means
62
Kco
STBPa
VTR information storing means
71
STBPa (Kco)
MUX
54
Recording means
55
DMUX
57
Reproducing means
58
6
Recording medium

Fig. 16

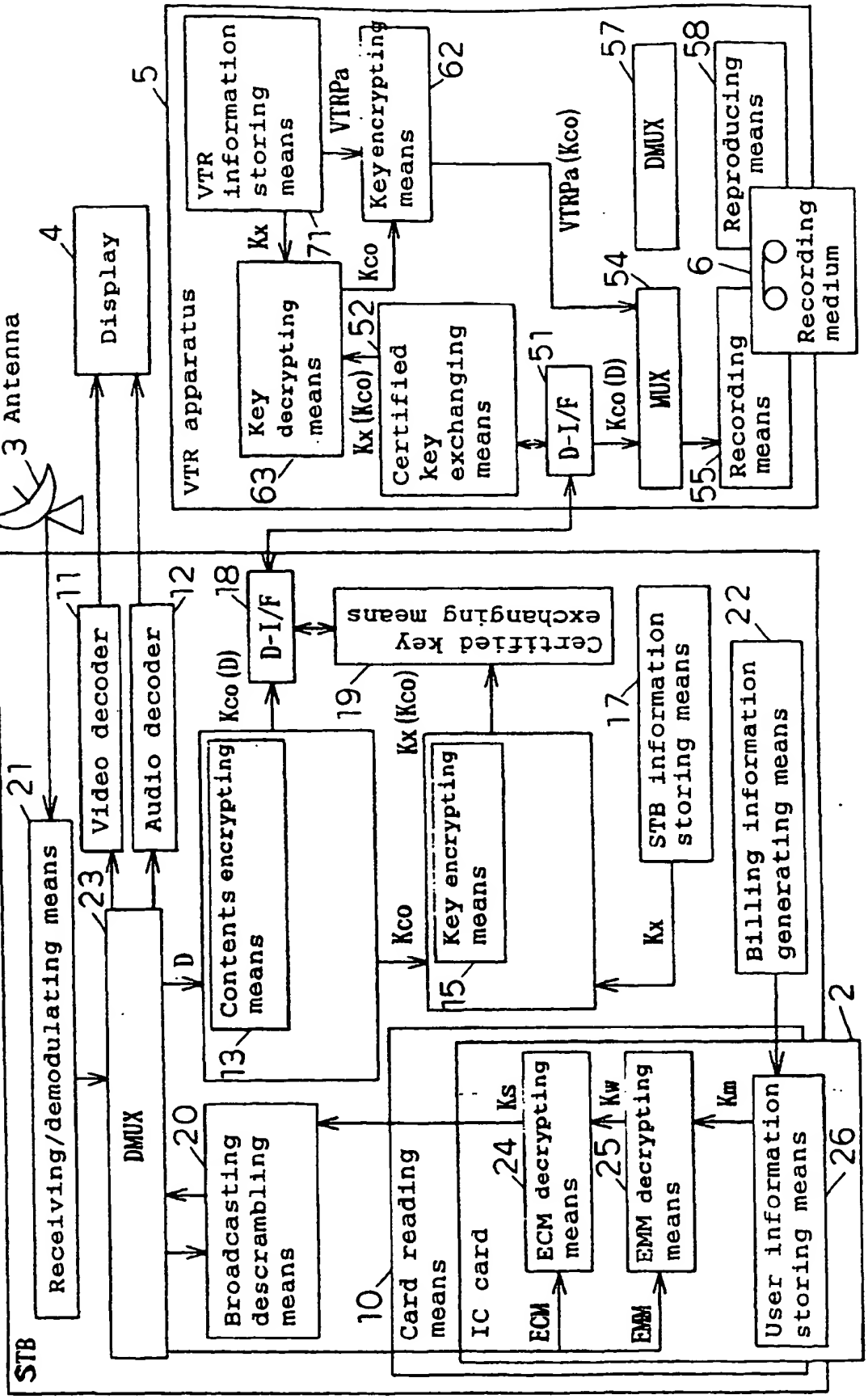

STB
Receiving/demodulating means
21
Video decoder
11
Audio decoder
12
DMUX
23
D
Broadcasting descrambling means
20
Kco (D)
D-I/F
18
Contents encrypting means
13
Kco
Key encrypting means
15
Kx (Kco)
Certified key exchanging means
19
Kx
STB information storing means
17
Billing information generating means
22
2
Card reading means
10
IC card
ECM
ECM decrypting means
24
Ks
EMM
EMM decrypting means
25
Kw
Km
User information storing means
26
3 Antenna
4
Display
5
VTR apparatus
VTR information storing means
71
VTRPa
Key encrypting means
62
Kx
Kco
Key decrypting means
63
Kx (Kco)
52
Certified key exchanging means
51
D-I/F
Kco (D)
MUX
54
VTRPa (Kco)
DMUX
57
Reproducing means
58
6
Recording means
55
Recording medium

Fig. 18

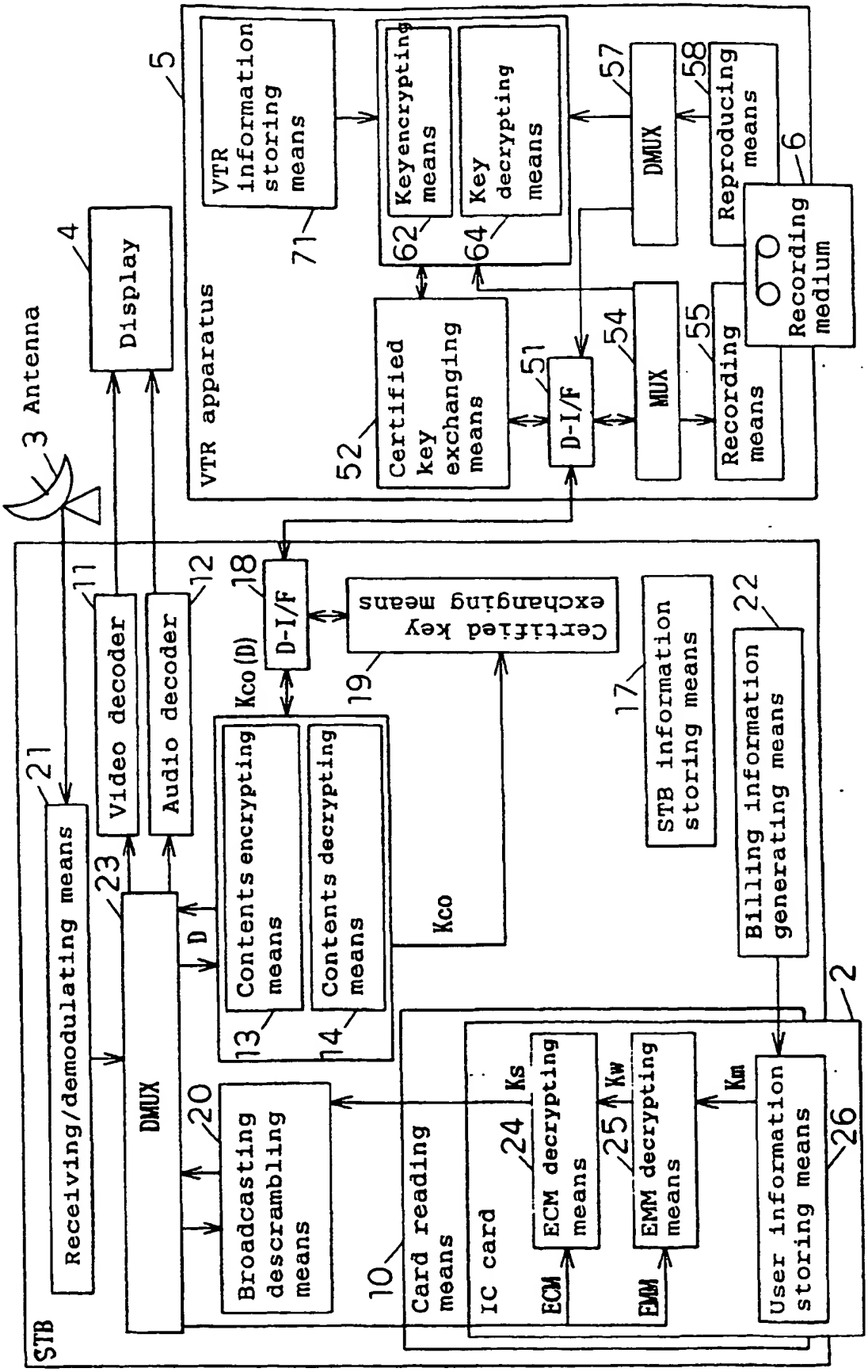

STB
Receiving/demodulating means
21
DMUX
23
Video decoder
11
Audio decoder
12
Broadcasting descrambling means
20
D
Contents encrypting means
13
Contents decrypting means
14
Kco (D)
D-I/F
18
Certified key exchanging means
19
Kco
Card reading means
10
IC card
ECM decrypting means
24
Ks
ECM
EMM decrypting means
25
Kw
EMM
Km
User information storing means
26
STB information storing means
17
Billing information generating means
22
2
3 Antenna
4
Display
5
VTR apparatus
VTR information storing means
71
Keyencrypting means
62
Key decrypting means
64
Certified key exchanging means
52
D-I/F
51
MUX
54
Recording means
55
DMUX
57
Reproducing means
58
Recording medium
6

Fig. 20

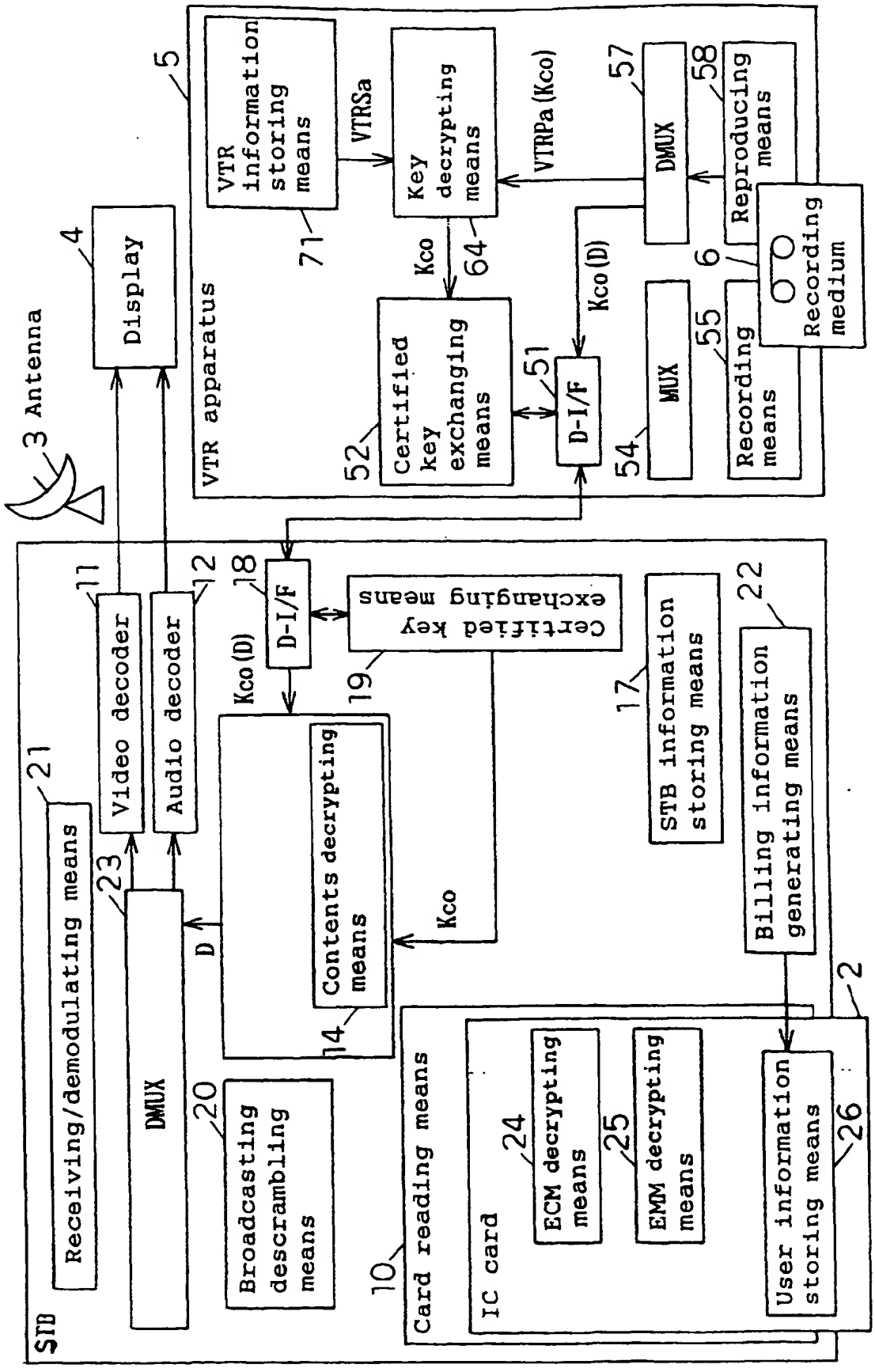

STB
Receiving/demodulating means
21
Video decoder
11
Audio decoder
12
DMUX
23
D
Broadcasting descrambling means
20
Kco(D)
D-I/F
18
Certified key exchanging means
19
Contents decrypting means
14
Kco
Card reading means
10
IC card
ECM decrypting means
24
EMM decrypting means
25
User information storing means
26
STB information storing means
17
Billing information generating means
22
2
3 Antenna
4
Display
5
VTR apparatus
VTR information storing means
71
VTRSa
Key decrypting means
64
VTRPa (Kco)
Kco
Kco(D)
DMUX
57
Reproducing means
58
6
Recording means
55
Recording medium
MUX
54
D-I/F
51
Certified key exchanging means
52

Fig. 22

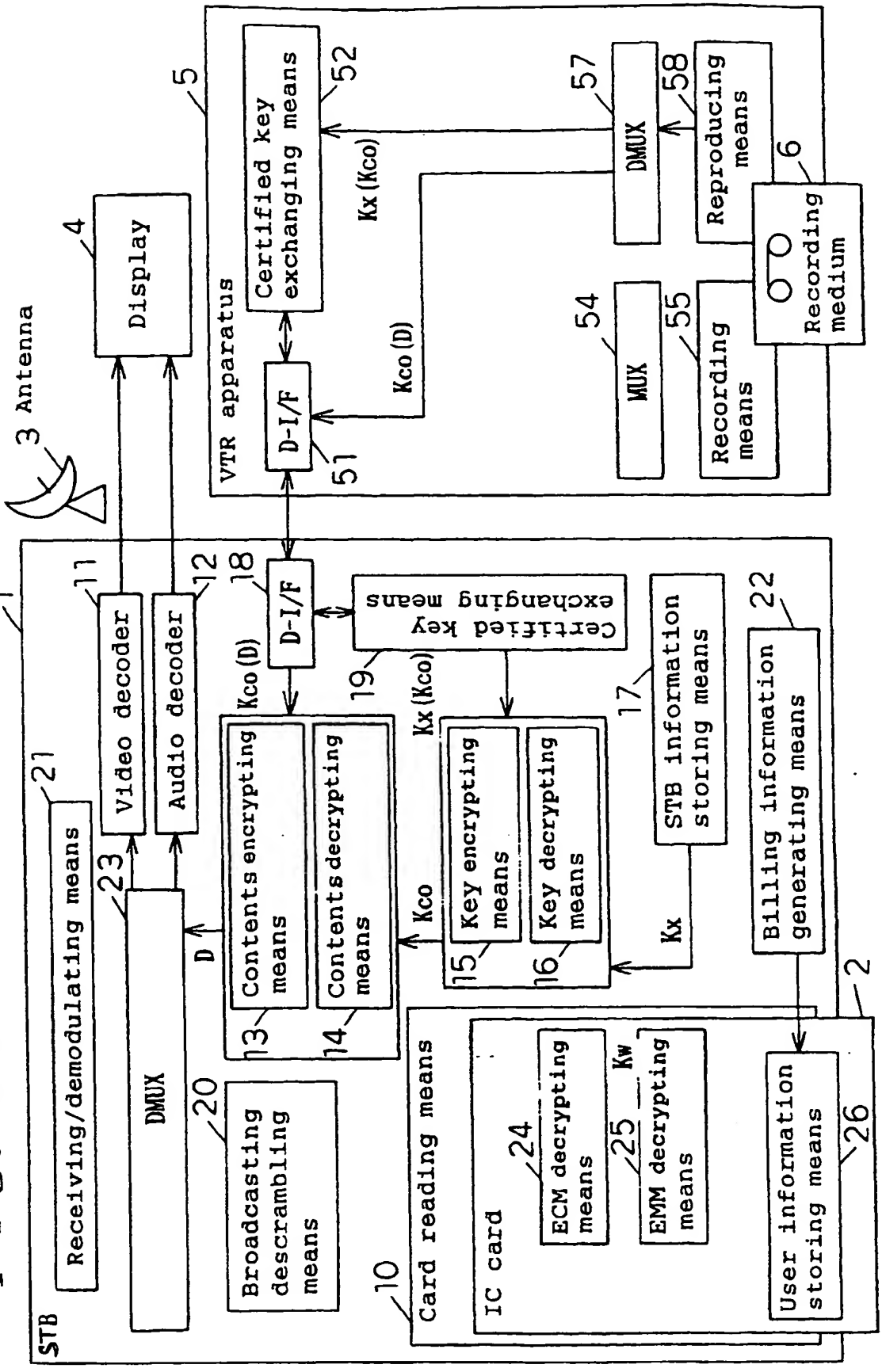

STB
1
Receiving/demodulating means
21
Video decoder
11
Audio decoder
12
DMUX
23
20
Broadcasting descrambling means
D
Contents encrypting means
13
Contents decrypting means
14
Kco (D)
D-I/F
18
Certified key exchanging means
19
Kx (Kco)
Kco
Key encrypting means
15
Key decrypting means
16
Kx
STB information storing means
17
Billing information generating means
22
2
Card reading means
10
IC card
ECM decrypting means
24
Kw
EMM decrypting means
25
User information storing means
26
3 Antenna
4
Display
5
VTR apparatus
Certified key exchanging means
52
D-I/F
51
Kco (D)
Kx (Kco)
DMUX
57
58
Reproducing means
6
Recording medium
MUX
54
Recording means
55

Fig. 24

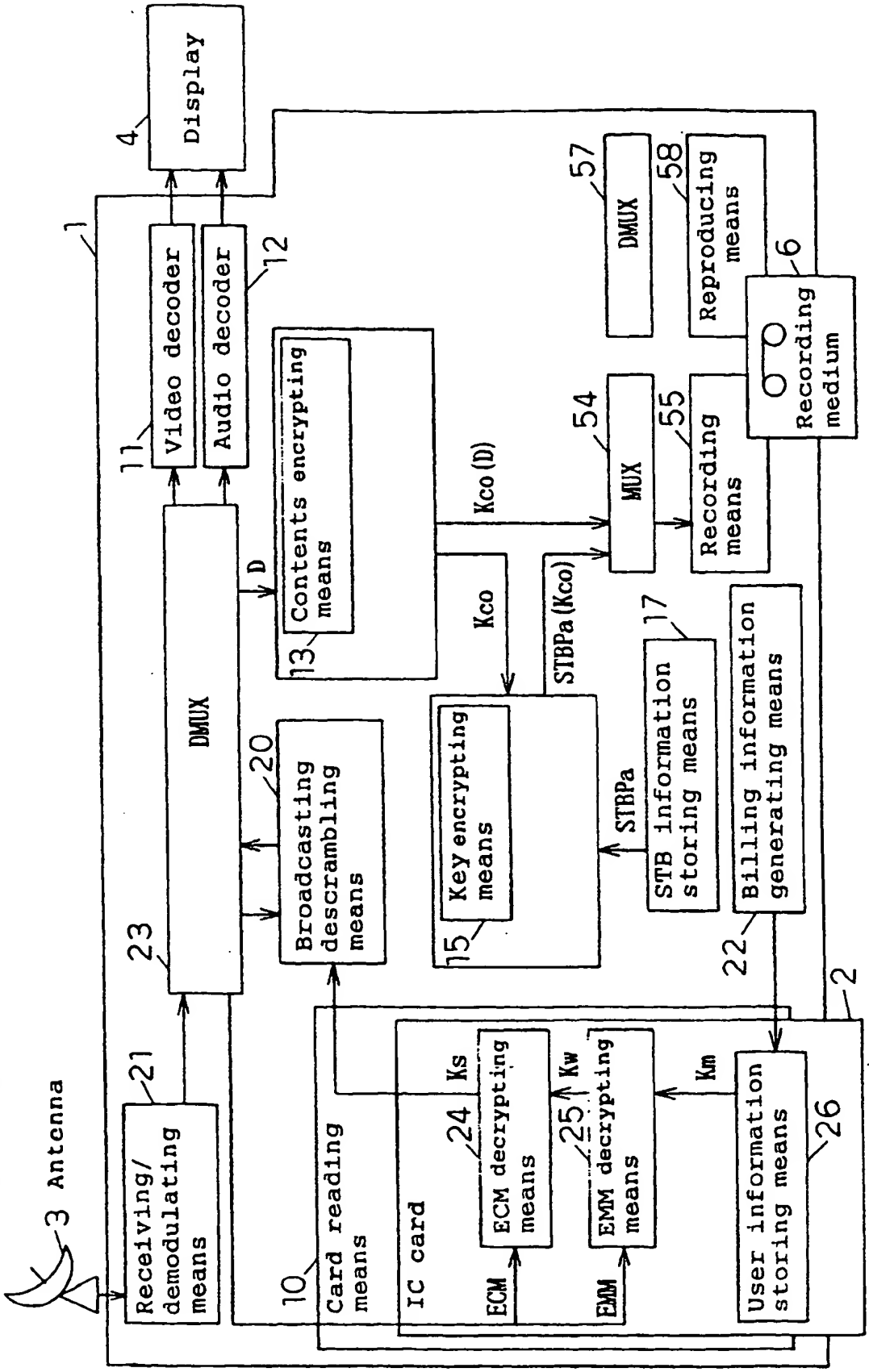

3 Antenna
Receiving/ demodulating means
21
23
DMUX
Video decoder
11
Audio decoder
12
Display
4
1
D
Contents encrypting means
13
Kco (D)
Kco
STBPa (Kco)
Broadcasting descrambling means
20
Key encrypting means
15
STBPa
STB information storing means
17
Billing information generating means
22
MUX
54
Recording means
55
DMUX
57
Reproducing means
58
Recording medium
6
2
Card reading means
10
IC card
Ks
Kw
Km
ECM decrypting means
24
EMM decrypting means
25
ECM
EMM
User information storing means
26

Fig. 26

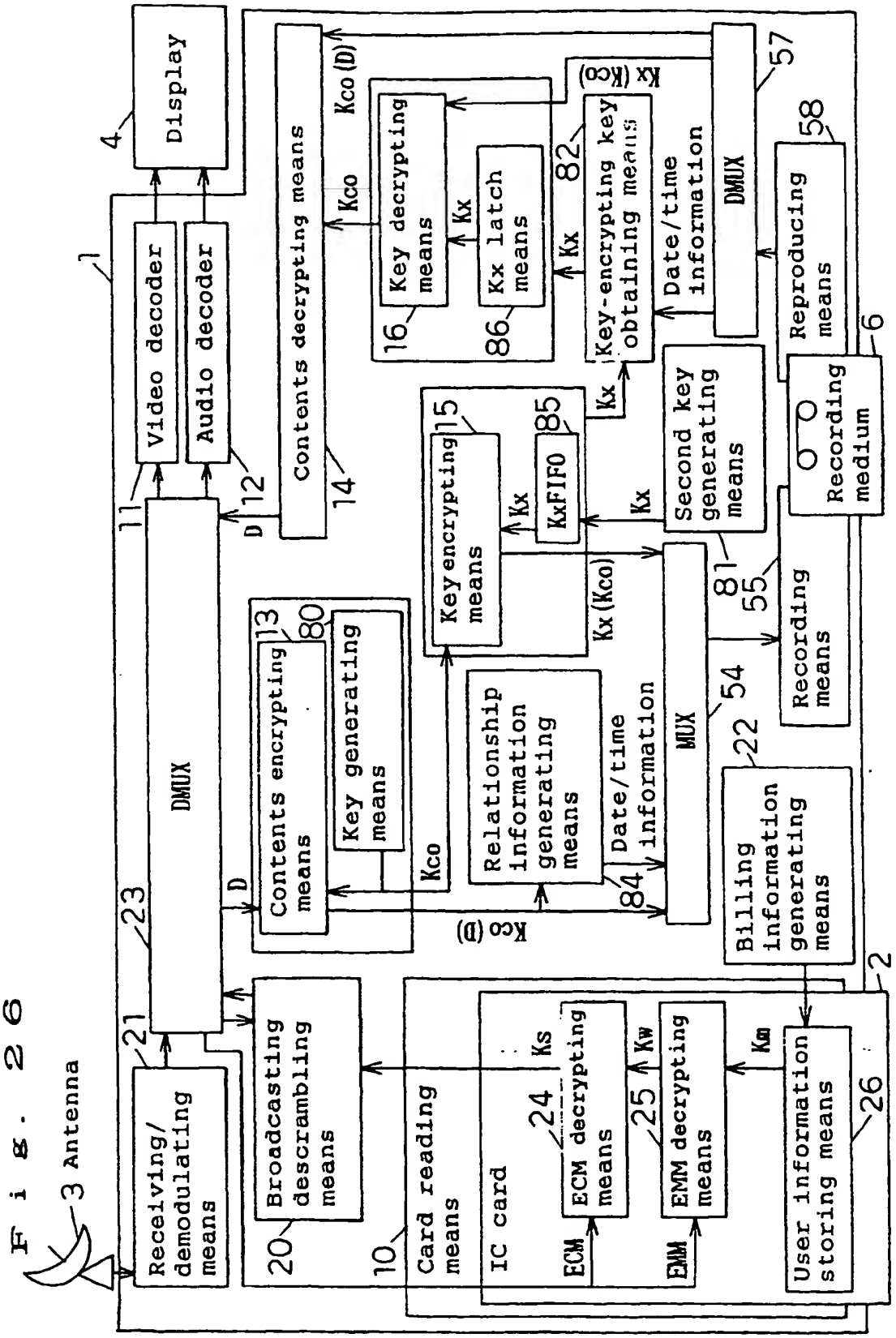

3 Antenna
Receiving/demodulating means
21
DMUX
23
Video decoder
Audio decoder
11
12
D
Display
4
1
Broadcasting descrambling means
20
Card reading means
10
IC card
Ks
ECM decrypting means
24
Kw
ECM
EMM decrypting means
25
Km
EMM
User information storing means
26
2
Contents encrypting means
13
Key generating means
80
Kco
D
Contents decrypting means
14
Kco (D)
Kco
Key decrypting means
16
Kx
Kx latch means
86
Kx
Key-encrypting key obtaining means
82
Kx (Kco)
Date/time information
DMUX
57
Reproducing means
58
Key encrypting means
15
Kx
KxFIFO
85
Kx
Kx (Kco)
Second key generating means
81
Recording means
55
Recording medium
6
Relationship information generating means
Date/time information
84
Kc (ID)
MUX
54
Billing information generating means
22

Fig. 28

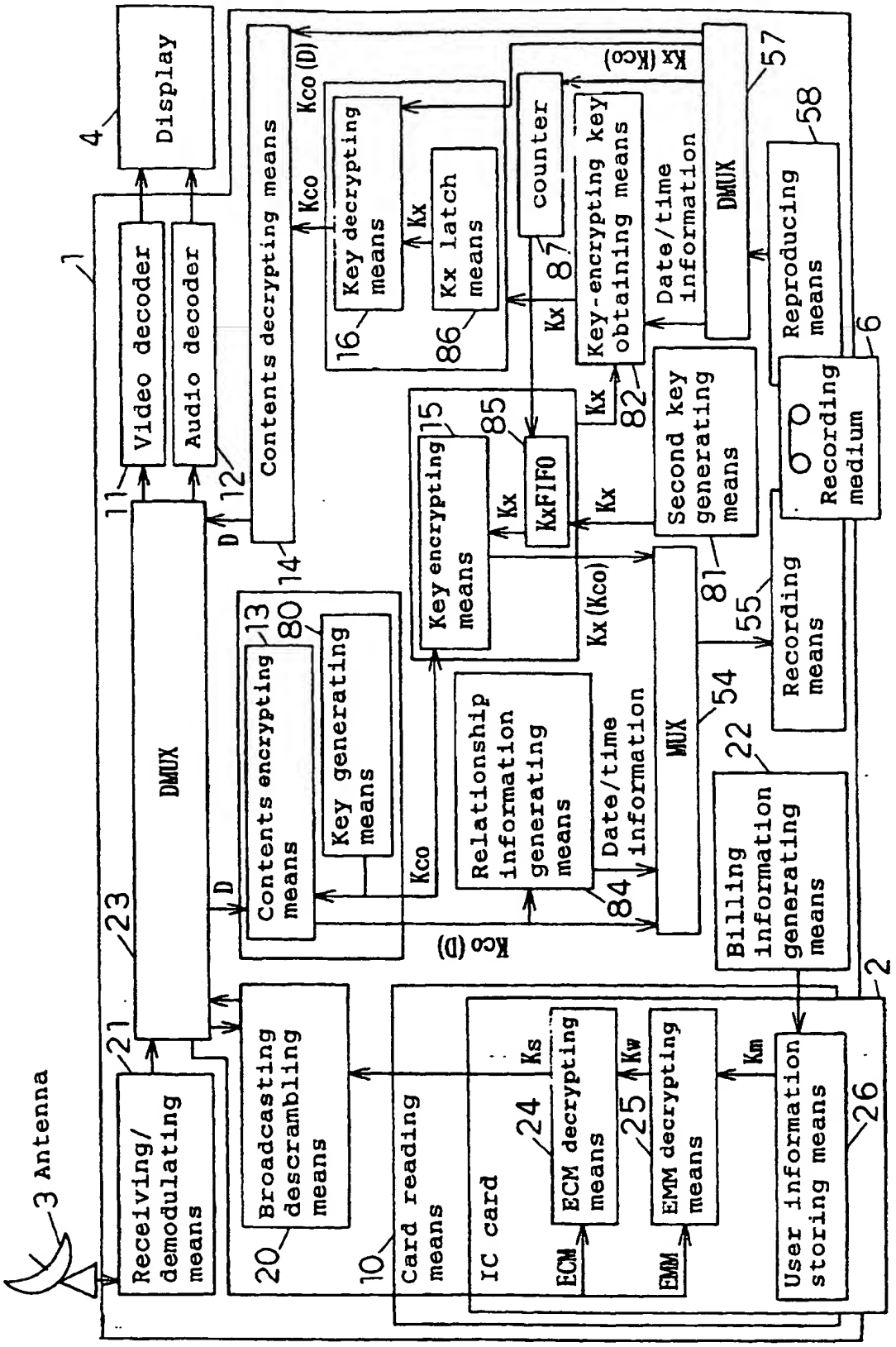
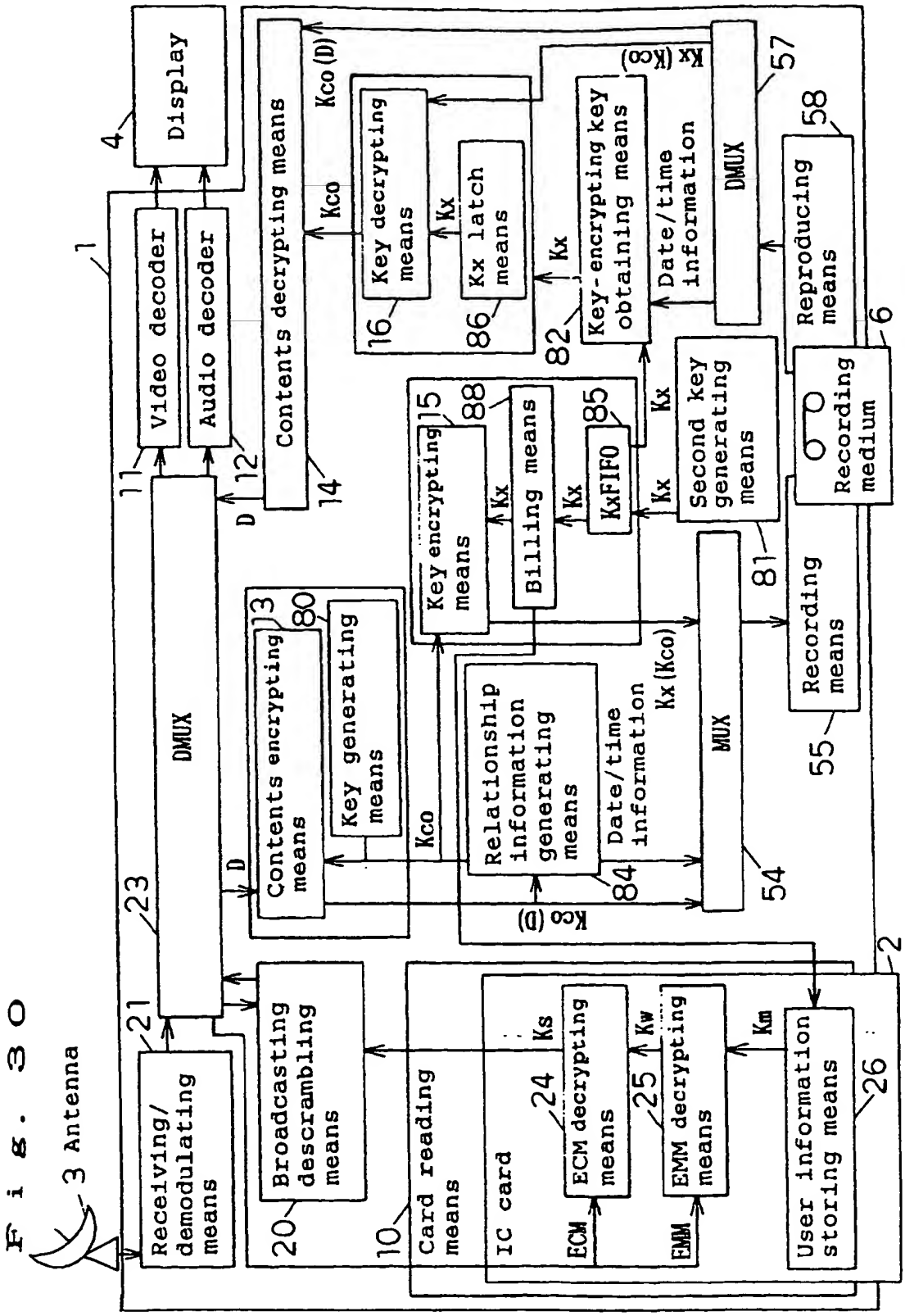

3 Antenna
Receiving/ demodulating means
21
DMUX
23
Video decoder
Audio decoder
11
Display
4
1
Broadcasting descrambling means
20
Card reading means
10
IC card
ECM
EMM
ECM decrypting means
24
EMM decrypting means
25
Ks
Kw
Km
User information storing means
26
2
Billing information generating means
22
MUX
54
Recording means
55
Recording medium
6
Reproducing means
58
DMUX
57
Second key generating means
81
Key-encrypting key obtaining means
82
Date/time information
counter
87
Kx (Kco)
Kx
Kco (D)
Contents decrypting means
12
D
14
Key decrypting means
16
Kx latch means
86
Kco
Contents encrypting means
13
Key generating means
80
Key encrypting means
15
KxFIFO
85
Kx
Kx (Kco)
Relationship information generating means
84
Date/time information
Kco (D)

Fig. 30


3 Antenna
Receiving/demodulating means
21
DMUX
23
Video decoder
Audio decoder
11
12
D
Display
4
1
Broadcasting descrambling means
20
Card reading means
10
IC card
ECM decrypting means
24
EMM decrypting means
25
ECM
EMM
Ks
Kw
Km
User information storing means
26
2
Contents encrypting means
13
Key generating means
80
Kco
D
Contents decrypting means
14
Kco (D)
Key decrypting means
16
Kx latch means
86
Kx
Key-encrypting key obtaining means
82
Kx (Kco)
Date/time information
DMUX
57
Reproducing means
58
Recording medium
6
Key encrypting means
15
Billing means
88
KxFIFO
85
Second key generating means
81
Recording means
55
Relationship information generating means
84
Date/time information
Kx (Kco)
MUX
54
Kc (D)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP99/00292

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[6] G11B20/10, H04N5/91

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[6] G11B20/10, H04N5/91

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1922-1996 Toroku Jitsuyo Shinan Koho 1994-1999
Kokai Jitsuyo Shinan Koho 1971-1999 Jitsuyo Shinan Toroku Koho 1996-1999

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X Y A	JP, 7-272399, A (Hitachi,Ltd.), 20 October, 1995 (20. 10. 95), Full text ; Figs. 1 to 18 Full text ; Figs. 1 to 18 Full text ; Figs. 1 to 18 (Family: none)	1, 4, 6 2, 3, 5 7-66
A	JP, 7-288798, A (Mitsubishi Electric Corp.), 31 October, 1995 (31. 10. 95), Full text ; Figs. 1 to 10 (Family: none)	11-14, 21
A	JP, 9-214929, A (Toshiba Corp.), 15 August, 1997 (15. 08. 97), Full text ; Figs. 1 to 6 (Family: none)	22-28
A	JP, 8-77706, A (Sony Corp.), 22 March, 1996 (22. 03. 96), Full text ; Figs. 1 to 7 (Family: none)	39-62

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
19 April, 1999 (19. 04. 99)	27 April, 1999 (27. 04. 99)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

Form PCT/ISA/210 (second sheet) (July 1992)